



# Department of Justice

February 2017  
WWW.JUSTICE.GOV

NSD  
(202) 514-2007

## **SUMMARY OF MAJOR U.S. EXPORT ENFORCEMENT, ECONOMIC ESPIONAGE, TRADE SECRET AND EMBARGO-RELATED CRIMINAL CASES** **(January 2014 to the present: updated February 17, 2017)**

Below is a brief description of some of the major export enforcement, economic espionage, theft of trade secrets, and embargo-related criminal prosecutions by the Justice Department since January 2014. These cases resulted from investigations by the Homeland Security Investigations (HSI) [formerly Immigration and Customs Enforcement (ICE)], the Federal Bureau of Investigation (FBI), the Department of Commerce's Bureau of Industry and Security (BIS), the Pentagon's Defense Criminal Investigative Service (DCIS), and other law enforcement agencies. This list of cases is not exhaustive and only represents select cases.

***Production and Development of Nuclear Material for China*** – On Jan. 6, 2017, in the Eastern District of Tennessee, Szuhsiung Ho, aka Allen Ho, a naturalized U.S. citizen, pleaded guilty to conspiracy to unlawfully engage or participate in the production or development of special nuclear material outside the U.S., without the required authorization from the U.S. Department of Energy (DOE), in violation of the Atomic Energy Act. In Apr. 2016, a federal grand jury issued a two-count indictment against Ho; China General Nuclear Power Company (CGNPC), the largest nuclear power company in China; and Energy Technology International (ETI), a Delaware corporation. At the time of the indictment Ho was a nuclear engineer, employed as a consultant by CGNPC, and was also the owner of ETI. CGNPC specialized in the development and manufacture of nuclear reactors and was controlled by China's State-Owned Assets Supervision and Administration Commission. According to documents filed in the case, beginning in 1997 and continuing through Apr. 2016, Ho conspired with others to engage or participate in the development or production of special nuclear material in China, without specific authorization to do so from the U.S. Secretary of Energy, as required by law. Ho assisted CGNPC in procuring U.S.-based nuclear engineers to assist CGNPC and its subsidiaries with designing and manufacturing certain components for nuclear reactors more quickly by reducing the time and financial costs of research and development of nuclear technology. In particular, Ho sought technical assistance related to CGNPC's Small Modular Reactor Program; CGNPC's Advanced Fuel Assembly Program; CGNPC's Fixed In-Core Detector System; and verification and validation of nuclear reactor-related computer codes. Under the direction of CGNPC, Ho also identified, recruited, and executed contracts with U.S.-based experts from the civil nuclear industry who provided technical assistance related to the development and production of special nuclear material for CGNPC in China. Ho and CGNPC also facilitated travel to China for and payments to the U.S.-based experts in exchange for their services. This investigation was conducted by the FBI, Tennessee Valley Authority-Office of the Inspector General, DOE-National Nuclear Security Administration and U.S. Immigration and Customs Enforcement Homeland Security Investigations, with assistance from other agencies.

***Munitions to Egypt*** – On Dec. 16, 2016, AMA United Group, Malak Neseem Swares Boulos and Amged Kamel Yonan Tawdraus were each sentenced in the Eastern District of New York after pleading guilty on Apr. 1, 2015, to violating the Arms Export Control Act, in connection with the attempted shipment of munitions samples from New York City to Egypt. AMA United Group, an Egyptian procurement agent, entered a guilty plea to violating the Arms Export Control Act. Boulos and Tawdraus, Egyptian citizens and partners in AMA United Group, pleaded guilty to failing to file required export information relating to the international shipment of a landmine and multiple bomblet bodies. AMA United Group was sentenced to one year of probation and \$400 special assessment. Boulos and Tawdraus were each sentenced to three years and six months home confinement, \$100 special assessment and a fine of \$2,500. According to court filings and facts presented during the plea proceeding, Boulos and Tawdraus were arrested after attempting to close a deal to acquire and export the items, which were included on the U.S. Munitions List and regulated by the U.S. Department of State. Beginning in Feb. 2011, the defendants began trying to obtain munitions items on behalf of AMA United Group’s client, a factory in Cairo. The items the defendants sought included a landmine as well as bomblet bodies and “trumpet liners,” two components that are integral to manufacturing the housings for explosives in an aerial warhead. In Jul. 2011, the defendants traveled from Cairo to New York City to inspect the items. On Jul. 1, 2011, the three principals of AMA United Group attempted to ship samples to its client in Egypt. Boulos and Tawdraus failed to file any export information in connection with the attempted shipment. The requirement to file accurate information regarding the contents of international shipments is one layer of regulatory oversight pertaining to protecting the U.S. national security and diplomatic interests. This case was investigated by the U.S. Immigration and Customs Enforcement’s Homeland Security Investigations (ICE-HSI) and the Defense Criminal Investigative Service (DCIS).

***Theft of Trade Secrets for Technologically Advanced Titanium to China*** – On Dec. 16, 2016, in the District of Connecticut, Yu Long, a citizen of China and lawful permanent resident of the U.S., waived his right to be indicted and pleaded guilty to charges related to his theft of numerous sensitive military program documents from United Technologies and transporting them to China. Long pleaded guilty to one count of conspiracy to engage in the theft of trade secrets knowing that the offense would benefit a foreign government, foreign instrumentality or foreign agent. He also pleaded guilty to one count of unlawful export and attempted export of defense articles from the U.S., in violation of the Arms Export Control Act. Previously, on Nov. 7, 2014, Long was arrested in Ithaca, NY, pursuant to a federal criminal complaint which charged Long with attempting to travel to China with sensitive proprietary documents that set forth detailed equations and test results used in the development of technologically advanced titanium for U.S. military aircraft. The documents were taken from a Connecticut defense contractor where Long had been employed. Long attempted, two days earlier, to fly to China from Newark Liberty International Airport in New Jersey. As alleged in the complaint affidavit and in statements made in court, Long holds Chinese citizenship and is a lawful permanent resident of the U.S. From approximately Aug. 2008, to May 2014, Long worked as a Senior Engineer/Scientist at a research and development center for a major defense contractor in Connecticut (“Company A”). Both during and after his employment there, Long traveled to the People’s Republic of China. Most recently, on Aug. 19, 2014, Long returned to the U.S. from China through John F. Kennedy International Airport in New York. During a secondary inspection screening by U.S. Customs and Border Protection (CBP) officers, Long was found in the possession of \$10,000.00 in undeclared U.S. cash, registration documents for a new corporation being set up in China, and a largely completed application for work with a state-controlled aviation and aerospace research center in China. The application materials highlighted certain of Long’s work history and experiences that he claimed to have obtained while employed at Company A, including work on F119 and F135 engines. The F119 engine is employed by the U.S. Air Force F-22 Raptor fighter

aircraft. The F135 engine is employed by the U.S. Air Force F-35 Lightning II fighter aircraft. The criminal complaint and statements made in court further state that on Nov. 5, 2014, Long boarded a flight from Ithaca to Newark Liberty International Airport, with a final destination of China. During Long's layover in Newark, CBP officers inspected Long's checked baggage and discovered that it contained, among other things, sensitive, proprietary and export controlled documents from another major defense contractor located outside the state of Connecticut ("Company B"). Further investigation determined that the U.S. Air Force had convened a consortium of major defense contractors, including Company A and Company B, to work together to see whether they could collectively lower the costs of certain metals used. As part of those efforts, members of the consortium shared technical data, subject to stringent restrictions on further dissemination. Company B reviewed the Company B documents found in Long's possession at Newark Liberty Airport and confirmed that it provided the documents to Company A as part of the consortium. Company B further confirmed that Long was never an employee of Company B. A review of Company A's computer records indicated that Long had printed the documents while employed at Company A. The documents bore warnings that they contained sensitive, proprietary and export-controlled material, which could not be copied or communicated to a third party. This investigation was conducted by the FBI, HSI, and CBP.

***Prohibited Financial Transactions in Iran*** – On Dec. 15, 2016, in the District of Alaska, Kenneth Zong was named as the sole defendant in the 47-count indictment charging him with conspiracy to violate the International Emergency Economic Powers Act (IEEPA), unlawful provision of services to Iran, money laundering conspiracy and money laundering. The indictment alleged that at an undetermined time, Zong left Alaska for Seoul, South Korea, and operated businesses there. From Jan. 2011, through at least Apr. 2014, Zong and four co-conspirators – three Iranian nationals and one U.S. citizen – allegedly conspired to evade the prohibitions of IEEPA and Iranian Transactions and Sanctions Regulations (ITSR) by engaging in false, fictitious and fraudulent transactions which were designed to unlawfully convert and remove Iranian owned funds, equivalent to approximately \$1 billion United States dollars (USD). These funds were held in controlled Korean bank accounts and converted into more easily tradeable currencies, such as dollars and/or euros, by defrauding the Korean regulators into thinking the transactions were legitimate. Zong is charged with transferring those currencies to more than 10 countries around the world, including the U.S., United Arab Emirates, Switzerland, Germany, Austria and Italy. Zong received payment for these acts from the Iranian nationals in an amount from \$10 million to \$17 million USD. The indictment alleged that the scheme began in 2011, when Zong changed the name of his Korean company, "KSI Ejder, Inc." (KSI) to "Anchore." Zong used KSI/Anchore as a conduit to convert and distribute Iranian funds into USD and/or euros, by fictitiously selling marble tiles and other construction supplies to an Iranian shell company in Kish Island, Iran. KSI/Anchore fictitiously purchased Italian marble tiles and other construction supplies from "MSL & Co Investment Trading" (MSL Investment Dubai), an Iranian-controlled shell company in Dubai, which were then fictitiously shipped directly to another fictitious company in Iran. Zong and his co-conspirators created false and fictitious contracts, bills of lading and invoices to show Korean government banking regulators that the Iranian company owed KSI/Anchore for the false marble purchases. This resulted in the transfer of Iranian funds, at the direction of Zong's co-conspirators, from the restricted Iranian bank account to Zong's KSI/Anchore account. Zong then transferred the funds to entities and individuals throughout the world. Zong is also charged with 43 counts of money laundering and one count of money laundering conspiracy for his actions in connection with the \$10 million fee paid to him by his Iranian associates. In furtherance of the scheme, Zong transferred \$10 million of his fees from Korea to a co-conspirator who resided in Anchorage. This individual also created and operated various companies to be used as front companies to purchase real estate, automobiles, an interest in a yacht and other purchases or transfers of the Iranian funds. The U.S.

embargo on Iran, which is enforced through IEEPA and the ITSR, prohibits the export of goods, technology, and services to Iran with very limited exceptions. This case was investigated by the IRS-Criminal Investigation and the FBI.

***Components for IEDs to Iran and Iraq*** – On Dec. 15, 2016, in the District of Columbia, Lim Yong Nam, aka Steven Lim, a citizen of Singapore, pleaded guilty to a federal charge stemming from his role in a conspiracy that allegedly caused thousands of radio frequency modules to be illegally exported from the U.S. to Iran. At least 16 of the components were later found in unexploded improvised explosive devices (IEDs) in Iraq. Lim was extradited earlier this year from Indonesia, where he had been detained since Oct. 2014, in connection with the U.S. request for extradition. He pleaded guilty to a charge of conspiracy to defraud the U.S. by dishonest means. The charge carries a statutory maximum of five years in prison and potential financial penalties. Lim and others were indicted in the District of Columbia in Jun. 2010, on charges involving the shipment of radio frequency modules made by a Minnesota-based company. The modules have several commercial applications, including in wireless local area networks connecting printers and computers in office settings. These modules include encryption capabilities and have a range allowing them to transmit data wirelessly as far as 40 miles when configured with a high-gain antenna. These same modules also have potentially lethal applications. Notably, during 2008 and 2009, coalition forces in Iraq recovered numerous modules made by the Minnesota firm that had been utilized as part of the remote detonation system for IEDs. According to the plea documents filed, between 2001 and 2007, IEDs were the major source of American combat casualties in Iraq. In his guilty plea, Lim admitted that between Aug. 2007, and Feb. 2008, he and others caused 6,000 modules to be purchased and illegally exported from the Minnesota-based company through Singapore, and later to Iran, in five shipments, knowing that the export of U.S.-origin goods to Iran was a violation of U.S. law. In each transaction, Lim and others made misrepresentations and false statements to the Minnesota firm that Singapore was the final destination of the goods. At no point in the series of transactions did Lim or any of his co-conspirators inform the company that the modules were destined for Iran. Similarly, according to the statement of offense, Lim and others caused false documents to be filed with the U.S. government, in which they claimed that Singapore was the ultimate destination of the modules. Lim and his co-conspirators were directly aware of the restrictions on sending U.S.-origin goods to Iran. Shortly after the modules arrived in Singapore, they were kept in storage at a freight forwarding company until being aggregated with other electronic components and shipped to Iran. There is no indication that Lim or any of his co-conspirators ever took physical possession of these modules before they reached Iran or that they were incorporated into another product before being re-exported to Iran. According to the statement of offense, 14 of the 6,000 modules the defendants routed from Minnesota to Iran were later recovered in Iraq, where the modules were being used as part of IED remote detonation systems. This investigation was jointly conducted by ICE Homeland Security Investigations (HSI) and the Department of Commerce, Bureau of Industry and Security. Substantial assistance was provided by the U.S. Department of Defense, U.S. Customs and Border Protection, the State Department's Directorate of Defense Trade Controls, the Treasury Department's Office of Foreign Assets Control, and the Office of International Affairs in the Justice Department's Criminal Division, the Justice Department Attaché in the Philippines and the FBI and HSI Attachés in Singapore and Jakarta.

***Aviation Parts and Supplies to Iran*** – On Dec. 14, 2016, in the District of Columbia, Mansour Moghtaderi Zadeh, an Iranian national, was sentenced to 18 months in prison and one year of supervised release for taking part in a conspiracy involving the purchase and shipment of various products, including aviation parts and aviation supplies, from the U.S. to Iran without a license. Zadeh was also ordered to pay a forfeiture money judgment in the amount of \$69,159.00. Zadeh,

who had been living in Iran, pleaded guilty on Oct. 27, 2016, to one count of conspiracy to unlawfully export goods, technology and services to Iran without the required license, and to defraud the U.S., in violation of 18 U.S.C. § 371, 50 U.S.C. § 1705, and 31 C.F.R. Parts 560.203 and 560.204. In court documents filed at the time of the plea, Zadeh acknowledged that beginning in Oct. 2005, Iranian companies requested that Zadeh through his company, Barsan, procure products including a fiber optic video transmitter and receiver, and aviation course indicators that would otherwise require a license from the Office of Foreign Assets Control (OFAC) to be exported to Iran. Members of the conspiracy arranged for the items to be sent from the U.S. to Iran, for which Zadeh received a commission. In Mar. 2007, Zadeh and co-conspirators attempted to export metal sheets and rods that are used in the aviation manufacturing industry from the U.S. to Iran without the required license from OFAC. Zadeh had arranged for his new corporation, Lavantia, to purchase the items. Zadeh also used an alias in his communications. In Sep. 2007, the shipment was detained by the U.S. Department of Commerce pending certification of the end user. In Oct. 2007, the Department of Commerce issued a Temporary Denial Order (TDO) against Lavantia and Zadeh, under his alias. The TDO prohibited Lavantia and Zadeh from participating in any way in exporting commodities from the U.S. Notwithstanding the TDO, Zadeh and other conspirators exported and attempted to export numerous materials from the U.S., including resin, sealant, paint, pneumatic grease, film adhesive and polyurethane coating and thinner. The post-TDO conduct included more than \$69,000 of exported goods. This investigation was conducted by the U.S. Immigration and Customs Enforcement's Homeland Security Investigations, and the Bureau of Industry and Security at the U.S. Department of Commerce.

***Cutting-Edge Microelectronics to Russia*** – On Dec. 6, 2016, in the Eastern District of New York, Alexey Barysheff of Brooklyn, New York, a naturalized citizen of the United States, was arrested on federal charges of illegally exporting controlled technology from the United States to end-users in Russia. Simultaneously, two Russian nationals, Dmitri Aleksandrovich Karpenko and Alexey Krutinin, were arrested in Denver, Colorado, on charges of conspiring with Barysheff and others in the scheme. Federal agents also executed search warrants at two Brooklyn locations that were allegedly used as front companies in Barysheff's illegal scheme. Barysheff made his initial appearance on Dec. 6, 2016, in the Eastern District of New York. Karpenko and Krutinin made their initial appearances on Dec. 6, 2016, in the District of Colorado. On Dec. 18, 2016, the Court ordered their removal in custody to the Eastern District of New York. The complaints allege that Barysheff, Karpenko, Krutinin, and others were involved in a conspiracy to obtain cutting-edge microelectronics from manufacturers and suppliers located within the United States and to export those high-tech products to Russia, while evading the government licensing system set up to control such exports. The microelectronics shipped to Russia included, among other products, digital-to-analog converters and integrated circuits, which are frequently used in a wide range of military systems, including radar and surveillance systems, missile guidance systems and satellites. These electronic devices required a license from the Department of Commerce to be exported to Russia and have been restricted for anti-terrorism and national security reasons. As further detailed in the complaints, in 2015 Barysheff registered the Brooklyn, New York-based companies BKLN Spectra, Inc. (Spectra) and UIP Techno Corp. (UIP Techno). Since that time, the defendants and others have used those entities as U.S.-based front companies to purchase, attempt to purchase, and illegally export controlled technology. To induce U.S.-based manufacturers and suppliers to sell them high-tech, export-controlled microelectronics and to evade applicable controls, the defendants and their co-conspirators purported to be employees and representatives of Spectra and UIP Techno and provided false end-user information in connection with the purchase of the items, concealed the fact that they were exporters and falsely classified the goods they exported on records submitted to the Department of Commerce. To conceal the true destination of the controlled microelectronics from the U.S. suppliers, the defendants and

their co-conspirators shipped the items first to Finland and subsequently to Russia. This case was investigated by ICE-HSI, FBI, Department of Commerce-BIS, and DoD DCIS.

***Controlled Microelectronics to Russian Military and Intelligence Agencies*** – On Dec. 1, 2016, Shavkat Abdullaev was sentenced in the Eastern District of New York to 36 months' imprisonment, 2 years supervised release, and \$400 special assessment. Previously, on Jul. 21, 2016, Alexander Fishenko, a dual citizen of the United States and Russia, was sentenced to 120 months' imprisonment and ordered to forfeit more than \$500,000 in criminal proceeds following his guilty plea on Sept. 9, 2015, to a nineteen-count indictment. Fishenko was charged with acting as an agent of the Russian government within the United States without prior notification to the Attorney General, conspiring to export, and illegally exporting controlled microelectronics to Russia, conspiring to launder money, and obstruction of justice. Fishenko, ten other individuals, and two corporations – ARC Electronics, Inc. (ARC) and Apex System, L.L.C. (Apex) – were indicted in Oct. 2012. On Oct. 26, 2015, Alexander Posobilov, Shavkat Abdullaev and Anastasia Diatlova were convicted of all counts of the indictment. On Jan. 10, 2013, defendants Lyudmila Bagdikian and Viktoria Klebanova pleaded guilty for their roles in exporting goods from the United States to Russian end users. Three defendants remain at large. ARC is now defunct, and Apex, a Russian-based procurement firm, failed to appear in court. Previously, on Oct. 3, 2012, an indictment was unsealed in the Eastern District of New York charging 11 members of a Russian procurement network operating in the United States and Russia, as well as a Houston-based export company, Arc Electronics Inc., and a Moscow-based procurement firm, Apex System L.L.C., with illegally exporting high-tech microelectronics from the United States to Russian military and intelligence agencies. Fishenko, an owner and executive of both the American and Russian companies, was also charged with operating as an unregistered agent of the Russian government inside the U.S. by illegally procuring the microelectronics on behalf of the Russian government. The microelectronics allegedly exported to Russia are subject to U.S. controls due to their potential use in a wide range of military systems, including radar and surveillance systems, weapons guidance systems and detonation triggers. In conjunction with the unsealing of the charges, the Department of Commerce added 165 foreign persons and companies who received, transshipped, or otherwise facilitated the export of controlled commodities by the defendants to its "Entity List." As alleged in the indictment, between Oct. 2008, and the present, Fishenko and the other defendants engaged in a conspiracy to obtain advanced microelectronics from manufacturers and suppliers located in the United States and to export those high-tech goods to Russia, while evading the government export licensing system. The microelectronics shipped to Russia included analog-to-digital converters, static random access memory chips, microcontrollers and microprocessors. The defendants allegedly exported many of these goods, frequently through intermediary procurement firms, to Russian end users, including Russian military and intelligence agencies, and went to great lengths to conceal their procurement activities. The investigation uncovered a Russian Ministry of Defense document designating an Apex subsidiary as a company "certified" to procure and deliver military equipment and electronics. The FBI recovered a letter sent by a specialized electronics laboratory of Russia's Federal Security Service (FSB), Russia's primary domestic intelligence agency, to an Apex affiliate regarding certain microchips obtained for the FSB by Arc. The defendants' principal port of export for these goods was John F. Kennedy International Airport in New York. In addition to Fishenko, Arc, Apex, Posobilov, Abdullaev and Diatlova, the indictment also charged Sevinj Taghiyeva and Svetalina Zagon, who were arrested in Houston on Oct. 2 and Oct 3, 2012. Three others charged in the indictment, Sergey Klinov, Yuri Savin, and Dimitriy Shegurov, were based overseas and were not arrested. The investigation was conducted by the FBI, Department of Commerce (BIS), Naval Criminal Investigative Service (NCIS) and the IRS.

***Assault Rifles to Haiti*** – On Dec. 1, 2016, an indictment was returned in the Southern District of Florida charging both Samuel Baptiste and Jose Noel a.k.a. Abdul Jabar, a citizen of Haiti, with smuggling goods from the United States. The indictment also charged Noel with being an alien in possession of a firearm and Baptiste with being a felon in possession of a firearm. The investigation of Baptiste began in Apr. 2014, when investigating agents observed that Baptiste operated numerous social media accounts praising U.S. designated terrorists Usama bin Laden and Anwar Al-Awlaki, in addition to encouraging jihad and referencing becoming a martyr. The FBI assessed that Baptiste used his social media accounts since at least 2013 to disseminate extremist propaganda, to praise attacks conducted or inspired by Al Qaeda, and to promote travel to Syria for jihad. In mid-Oct. 2016, FBI agents launched an investigation of Noel based on information provided by a FBI Confidential Human Source (CHS). The CHS was first introduced to Noel through a mutual associate, Baptiste, in Oct. 2016. During a meeting between Baptiste, Noel and the CHS, Noel indicated a desire to obtain a T-56 rifle. Noel stated that he had previously obtained illegal guns from family members in Florida and further claimed to have transported concealed weapons to Haiti in the past. Noel also told the CHS about a security company he was trying to establish in Haiti and his desire to obtain guns for this company. During one of the meetings between the CHS, Baptiste and Noel, Noel advised the CHS that he (Noel) needed a 9mm handgun and also wanted to purchase an AR-15 assault rifle. On Nov. 5, 2016, Baptiste, Noel and the FBI CHS went to a shipping container acquired by the CHS. The CHS told Baptiste and Noel that the container was scheduled to be shipped to Haiti. Inside the container were FBI-acquired items that resembled relief items to be shipped to Haiti. Among the items were pallets of food, clothing, vehicle tires, and household appliances. Also placed inside the container concealed under clothing were two FBI-provided rifles – two Rock River Arms LAR-15 semi-automatic assault rifles – and four ammunition magazines for those rifles. The weapons were provided to Noel based on his requests to the FBI CHS to obtain AR-15-style rifles for him. Noel paid the CHS \$300 in case for one of the weapons. This case was investigated by the FBI.

***Sanctions Violations to Aid Iran*** – On Nov. 21, 2016, in the Eastern District of New York, Ahmad Sheikhzadeh, a U.S. citizen and resident of New York City, New York, pleaded guilty to filing a false income tax return that substantially understated the amount of cash salary the defendant received from Iran’s Permanent Mission to the United Nations (IMUN) and conspiring to facilitate the transfer of funds to Iran without the required license from the Treasury Department, in violation of the International Emergency Economic Powers Act (IEEPA). According to court filings and facts presented during the plea proceeding, beginning in Jan. 2008, Sheikhzadeh was employed as a consultant to the IMUN and received a regular salary, in cash, approximately once per month, through an intermediary who was an official at the IMUN. Sheikhzadeh was not a declared IMUN official. From 2008 through 2012, Sheikhzadeh filed personal income tax returns that substantially understated the amount of income he received from his work for the IMUN. In addition, distinct from his work for the IMUN, Sheikhzadeh provided money remitting (“hawala”) services to co-conspirators in the U.S. to facilitate investments in Iran and to direct disbursements from Iranian bank accounts. Sheikhzadeh engaged in these money transfers without a license from the Treasury Department’s Office of Foreign Assets Control, in violation of IEEPA. Sheikhzadeh will be sentenced on Mar. 30, 2017. When sentenced, the defendant faces up to 23 years in prison. The defendant has agreed to pay over \$147,000 in restitution and forfeiture. This case is investigated by the FBI and the IRS Criminal Investigation Division in New York.

***Integrated Circuits to China*** – On Nov. 4, 2016, in the District of Connecticut, Xianfeng Zuo of Shenzhen, China, was sentenced to 15 months of imprisonment for conspiring to sell counterfeits of sophisticated integrated circuits (ICs) to a purchaser in the U.S. According to court documents

and statements made in court, Zuo, Jiang Yan and Daofu Zhang each operated businesses in China that bought and sold electronic components, including ICs. In the summer of 2015, Zuo asked Yan to locate and purchase several advanced ICs made by Xilinx Corp., which had military applications, including radiation tolerance for uses in space. Yan then asked a U.S. individual to locate the Xilinx ICs and sell them to Yan. The U.S. individual explained that the ICs cannot be shipped outside the U.S. without an export license, but Yan still wished to make the purchase. When the U.S. individual expressed concern that the desired ICs would have to be stolen from military inventory, Yan proposed to supply the U.S. source with “fake” ICs that “look the same,” to replace the ones to be stolen from the military. In Nov. 2015, Zhang shipped from China to the U.S. individual, two packages containing a total of eight counterfeit ICs, each bearing a counterfeit Xilinx brand label. After further discussions between Yan and the U.S. individual, Yan, Zhang, and Zuo flew together from China to the U.S. in early Dec. 2015, to complete the Xilinx ICs purchase. On Dec. 10, 2015, the three conspirators drove to a location near Route 95 in Milford, Connecticut, where they planned to meet the U.S. individual, make payment, and take custody of the Xilinx ICs. Federal agents arrested all three at the meeting location. The defendants were charged under separate indictments in the District of Connecticut. On Mar. 7, 2016, Yan pleaded guilty both to conspiracy to traffic in counterfeit military equipment, in violation of 18 U.S.C. § 2320(a)(3); and to attempted, unlicensed export of advanced, export-restricted electronic equipment, in violation of the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701 et seq. Yan was sentenced on Dec. 29, 2016, to time-served. On Mar. 16, 2016, Zuo pleaded guilty to one count of conspiracy to traffic in counterfeit goods, in violation of 18 U.S.C. § 2320(a). On Apr. 15, 2016, Zhang also pleaded guilty to one count of conspiracy to traffic in counterfeit goods. Zhang was sentenced on Jul. 8, 2016, to 15 months of imprisonment. As part of their sentences, each defendant was ordered to forfeit his interest in the \$63,000 in cash seized incident to their arrests. This matter was investigated by the Defense Criminal Investigative Service, the Department of Homeland Security, the Department of Commerce, the Federal Bureau of Investigation, and the Air Force Office of Special Investigations.

***Firearm Parts to the Philippines*** – On Nov. 2, 2016, Kirby Santos of the Republic of the Philippines was sentenced in the District of New Jersey to 24 months’ imprisonment, 3 years supervised release, \$100 special assessment and \$2,400 fine after pleading guilty on Oct. 7, 2015, to an information charging him with one count of conspiracy to violate the Arms Export Control Act and U.S. anti-smuggling laws. According to the documents filed in this case, other cases and statements made in court: Santos admitted that from 2008 through Oct. 2013, he and conspirators he met in the Philippines or through an online forum agreed to ship firearms parts from the United States to the Philippines. Santos and others used credit cards and other forms of payment to purchase firearms parts from suppliers in the United States. Knowing that they would not ship to the Philippines, Santos arranged for the suppliers to send the firearms parts to the addresses of conspirators in Toms River, New Jersey, and Lynwood, Washington, in order to make the purchases appear as domestic sales. At the direction of Santos, the conspirators, including Abelardo Delmundo, 53, of Toms River, New Jersey, would then repackage the firearms parts, falsely label the contents of the package and export the firearms parts to the Philippines for ultimate delivery to Santos. To disguise their role in the conspiracy, the conspirators used aliases when sending the packages containing prohibited items. Upon receiving the firearms parts, Santos paid Delmundo and other conspirators in the form of cash or wire transfers to others at their direction. During the course of the nearly five-year long conspiracy, Santos and others purchased and directed the unlawful exportation of more than \$200,000 worth of defense articles from the United States to the Philippines without the required export license. Santos made his initial appearance in federal court on Apr. 22, 2015, after being charged by criminal complaint with one count of conspiracy to violate the Arms Export Control Act and U.S. anti-smuggling laws. The



Arms Export Control Act prohibits the export of defense articles and defense services without first obtaining a license from the U.S. Department of State and is one of the principal export control laws in the United States. Santos was arrested in Guam on Mar. 31, 2015, by special agents of the U.S. Department of Homeland Security-Homeland Security Investigations (DHS-HSI) and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF). Delmundo, charged in the District of New Jersey under a separate information, pleaded guilty to his role in the conspiracy on Apr. 30, 2015. This investigation was conducted by DHS-HSI, ATF.

***Firearms and Ammunition to Ghana*** – On Nov. 2, 2016, in the Western District of North Carolina, Richmond Akoto Attah was sentenced to 37 months of imprisonment, one year supervised release, and \$100 special assessment stemming from his plea of guilty on Jun. 7, 2016, to smuggling goods from the United States. On Feb. 16, 2016, a nine count indictment was returned charging Attah with one count of violating the Arms Export Control Act (AECA), one count of illegal firearms dealing, two counts of smuggling goods from the United States and four counts of making false statements to a firearms dealer. According to the indictment, beginning in at least 2013, Attah purchased numerous firearms and ammunition he intended to smuggle and illegally export to Ghana, West Africa. Attah obtained the firearms by misstating on the required federal forms that he was the actual buyer and transferee of the firearms. According to the indictment, Attah was not a federally licensed firearms dealer and did not possess a license to export firearms or ammunition to Ghana or any other country. The indictment further alleged that from on or about Sep. 2013, to Dec. 2015, Attah purchased approximately 63 firearms and 3,500 rounds of ammunition from various stores, internet vendors and at gun shows. On or about Sep. 4, 2015, Attah travelled from Charlotte to Ghana, returning on Oct. 10, 2015. During his return trip, Attah hid \$30,100 dollars in his luggage, falsely declaring on his customs paperwork that he was only bringing \$350 back into the United States. The indictment also alleged that from on or about Nov. 2015, to Dec. 13, 2015, Attah purchased approximately 22 firearms and ammunition from dealers in North Carolina and online. Attah then hid 27 firearms, including semi-automatic pistols and revolvers, inside a washing machine and a dryer, and 3,500 rounds of ammunition inside a barrel. Attah placed the washer, dryer, and barrel inside a shipping container and attempted to have it shipped from Charlotte to Ghana. According to court documents, U.S. Customs officers recovered the firearms and ammunition before they were shipped outside the United States. This case was investigated by ATF, FBI, ICE HSI and CBP.

***Military Aircraft Parts to Iran*** – On Oct. 26, 2016, in the Central District of California, Zavik Zargarian and Vache Nayirian were arrested on federal charges for their alleged role in a scheme to smuggle millions of dollars' worth of military aircraft parts and other potential defense items to Iran, in violation of the International Emergency Economic Powers Act (IEEPA) and the Iranian Transactions and Sanctions Regulations (ITSR). The defendants were taken into custody by special agents of U.S. Immigration and Customs Enforcement's HSI. The men are among five defendants charged in a nine-count federal indictment unsealed on Oct. 26, 2016, that alleged a conspiracy to purchase and ship more than \$3 million dollars' worth of jet fighter aircraft parts to Iran. Additionally, several of the defendants are accused of buying and illegally exporting fluorocarbon rubber O-rings to Iran. The O-rings in question have a variety of possible military applications, including use in aircraft hydraulic systems and landing gear. Also named in the indictment are Zargarian's Glendale-based company, ZNC Engineering, and two Iranian nationals, Hanri Terminassian, and Hormoz Nowrouz, both of whom are believed to be in Iran. The charges stem from a lengthy undercover probe spearheaded by HSI, with substantial assistance provided by the Defense Criminal Investigative Service and U.S. Customs and Border Protection (CBP). According to the indictment, Terminassian originally contacted Zargarian from Iran for assistance with obtaining military aircraft parts from U.S.-based suppliers. Subsequently, Zargarian negotiated on Terminassian's behalf to purchase the desired items from

an undercover HSI special agent who was posing as a parts supplier. The items included parts used in F-14, F-15, F-16 and F-18 fighter jets. Eventually, Terminassian traveled to the U.S. to meet with Zargarian and the undercover special agent to discuss the transaction. The indictment alleged the two men sought to purchase between 10 and 30 units of each item, with the total cost potentially exceeding \$3.6 million. The indictment also accuses Zargarian and Nayirian of conspiring with Terminassian and Nowrouz to export fluorocarbon rubber O-rings to Iran. The indictment alleged Terminassian contacted Nayirian and Zargarian on behalf of Nowrouz and sought their help to obtain the parts. Terminassian transferred funds for the purchase to Nayirian, who later provided the money to Zargarian. Through his company ZNC Engineering, Zargarian bought the O-rings from a California vendor and provided them to Nayirian. Nayirian then exported the O-rings to addresses in the United Arab Emirates and Kuwait provided by Terminassian, who subsequently arranged for them to be transshipped to Iran. According to the indictment, the defendants exported more than 7,000 O-rings to Iran over the course of the conspiracy. To reduce the likelihood of detection, the defendants falsely claimed on shipping documents that the O-rings were destined for countries other than Iran and substantially undervalued them to avoid having to file export forms that might prompt further inspection by CBP. As part of their probe, investigators obtained evidence that the O-rings were intended for the Iranian Air Force. Zargarian and Nayirian were arraigned on the indictment in federal court on Oct. 26, 2016. Both men entered not guilty pleas. This case was investigated by ICE-HSI.

***Protected Rice Seeds to China*** – On Oct. 26, 2016, in the Eastern District of Arkansas, Wengui Yan pleaded guilty to one count of making false statements to the FBI while working as a geneticist for the U.S. Department of Agriculture at the Dale Bumpers National Research Center in Stuttgart. Yan, a scientist who worked with rice, admitted that he knew about plans to steal samples and send them to China. In his plea, Yan admitted that on Aug. 7, 2013, agents of U.S. Customs and Border Protection found stolen seeds in the luggage of a group of visitors from China preparing to board a plane to return home. The group had visited the facility in Stuttgart. Yan admitted that before the Chinese group arrived, a co-defendant in Kansas had asked him for seeds and Yan had declined because the seeds were protected. The co-defendant told Yan about other individuals seeking to steal samples of the seeds. When the delegation came to Stuttgart, Yan traveled with them to a rice farm where he knew they would have an opportunity to steal seeds. After the theft, Yan denied knowing about the plans to steal the seeds or about the theft itself. Investigators also learned that Yan attempted to cover up a trip he made to China to visit the crops research institute that sent the delegation to the United States. Co-defendant Weiqiang Zhang is awaiting trial. This case was investigated by the FBI and CBP.

***Restricted Laboratory Equipment to Syria*** – On Oct. 25, 2016, in the Middle District of Pennsylvania, Ahmad Feras Diri of London, was sentenced to 37 months' imprisonment and \$100 special assessment after pleading guilty on Apr. 21, 2016, to conspiracy to export items from the United States. Diri will be deported once he has completed his sentence. On Oct. 13, 2016, Harold Rinko, a U.S. citizen, was sentenced to time served, 2 years supervised release, \$100 special assessment and a fine of \$2500, after pleading guilty on Sept. 16, 2014, to conspiracy to export items from the United States. Rinko is also required to wear an electronic monitor for twelve months. Previously, on Nov. 20, 2012, an indictment was returned in the Middle District of Pennsylvania charging Diri; Mowea Diri, Ahmad's brother and a citizen of Syria; d-Deri Contracting & Trading, a business located in Syria; and Rinko with criminal conspiracy, wire fraud, illegal export of goods, money laundering and false statements. On Mar. 14, 2013, Diri was arrested by the Metropolitan Police in London in connection with the charges in the indictment and was extradited to the United States by the United Kingdom on Nov. 12, 2015. Diri was arraigned on charges alleging a conspiracy to illegally export laboratory equipment, including items used to detect chemical warfare agents, from the United States to

Syria. The indictment alleged that from 2003 until Nov. 20, 2012, the three men conspired to export items from the United States through third party countries to customers in Syria without the required U.S. Commerce Department licenses. According to the indictment, the conspirators prepared false invoices that undervalued and mislabeled the goods being purchased and listed false information regarding the buyers' identity and geographic location. The indictment alleged that the items were to be shipped from the United States to Jordan, the United Arab Emirates and the United Kingdom, and thereafter transshipped to Syria. The indictment further states that the items allegedly included: a portable gas scanner used for detection of chemical warfare agents by civil defense, military, police and border control agencies; a handheld instrument for field detection and classification of chemical warfare agents and toxic industrial chemicals; a laboratory source for detection of chemical warfare agents and toxic industrial chemicals in research, public safety and industrial environments; a rubber mask for civil defense against chemicals and gases; a meter used to measure chemicals and their composition; flowmeters for measuring gas streams; a stirrer for mixing and testing liquid chemical compounds; industrial engines for use in oil and gas field operations; and a device used to accurately locate buried pipelines. Pursuant to regulations of the U.S. Department of Commerce's Export Administration, a license is required to export goods and services from the United States to Syria, excepting limited and certain categories of humanitarian food and medicine. This case was investigated by ICE-HSI and U.S. Commerce Department's Office of Export Enforcement.

***Firearm Parts to the Republic of Turkey*** – On Oct. 7, 2016, Hamza Kolsuz, a citizen of the Republic of Turkey, was sentenced in the Eastern District of Virginia to 30 months' imprisonment, 3 years supervised release and ordered to pay \$200 special assessment. Previously, on Jun. 24, 2016, the Court issued Findings of Fact and Conclusions of Law finding Kolsuz guilty of all three counts in the indictment pending against him. The Court's ruling followed a two-day bench trial on May 18-19, 2016. On Mar. 2, 2016, after having previously been charged in a Criminal Complaint, a grand jury in the Eastern District of Virginia returned a three-count indictment against Kolsuz, charging him with: (1) conspiring to violate the Arms Export Control Act (the "AECA") and 18 U.S.C. § 554(a), in violation of 18 U.S.C. § 371; (2) attempting to export defense articles on the United States Munitions List ("USML") without a license or other written authorization from the United States Department of State's Directorate of Defense Trade Controls (the "DDTC"), in violation of the AECA; and (3) attempting to smuggle goods out of the United States, in violation of 18 U.S.C. § 554(a). The charges stemmed from Kolsuz's attempt to export firearms parts—specifically, eighteen handgun barrels, twenty-two 9mm handgun magazines, four .45 caliber handgun magazines, one .357 caliber handgun magazine and one .22 caliber Glock caliber conversion kit—to the Republic of Turkey, and his involvement in a years-long conspiracy to export firearms parts to the Republic of Turkey. Kolsuz arrived in the United States at Miami International Airport on Jan. 25, 2016, on a B-2 visitor's visa. While in Florida, Kolsuz and one of his co-conspirators visited gun stores and a gun show where they purchased firearms parts. On Feb. 2, 2016, Kolsuz began his return trip to Istanbul, Republic of Turkey by checking in at Miami International Airport for a flight that took him to Cleveland Hopkins International Airport. He then checked in for a flight that was to take him and his checked luggage through Cleveland Hopkins International Airport and Washington Dulles International Airport before embarking for Istanbul, Republic of Turkey on Turkish Airlines. When Kolsuz arrived at Dulles, his luggage was searched and the firearms parts were discovered. The eighteen handgun barrels, twenty-two 9mm handgun magazines, four .45 caliber handgun magazines, one .357 caliber handgun magazine, and one .22 caliber Glock caliber conversion kit were and are each defense articles listed on the USML, and a license or other written authorization from the DDTC was and is therefore required for the firearms parts to be lawfully exported from the United States. However, Kolsuz and his co-conspirators have never registered with the DDTC, or applied to register with the DDTC, to export defense articles from

the United States, and they have never applied for and have never received any licenses or other written authorization from the DDTC to export defense articles from the United States. This case was investigated by the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations.

***Theft of Trade Secrets of Inbred Corn Seeds to China*** – On Oct. 5, 2016, in the Southern District of Iowa, Mo Hailong, a/k/a Robert Mo, a Chinese national, was sentenced to 36 months in prison for conspiracy to steal trade secrets. Mo Hailong was also ordered to serve three years of supervised release following his term of imprisonment. On Dec. 19, 2016, Mo Hailong was ordered to pay restitution in the amount of \$425,000. In addition, the Court ordered the forfeiture of two farms in Iowa and Illinois that were purchased and utilized by Mo Hailong and others during the course of the conspiracy. Mo Hailong is a Chinese national who became a lawful permanent resident of the United States. During the course of the conspiracy, Mo Hailong was employed as the Director of International Business of the Beijing Dabeinong Technology Group Company, commonly referred to as DBN. DBN is a Chinese conglomerate with a corn seed subsidiary company, Kings Nower Seed. According to the plea agreement entered on Jan. 27, 2016, Mo Hailong admitted to participating in a long-term conspiracy to steal trade secrets from DuPont Pioneer and Monsanto. Mo Hailong participated in the theft of inbred corn seeds from fields in the Southern District of Iowa and elsewhere for the purpose of transporting the seeds to DBN in China. The stolen inbred, or parent, seeds were the valuable trade secrets of DuPont Pioneer and Monsanto. The investigation was initiated when DuPont Pioneer security staff detected suspicious activity and alerted the FBI. DuPont Pioneer and Monsanto were fully cooperative throughout the investigation. This matter was investigated by the FBI.

***Sanctions Violations to Aid North Korea's Nuclear Weapons and Ballistic Missile Programs*** – On Sept. 26, 2016, a criminal complaint was unsealed in the District of New Jersey charging four Chinese nationals and a trading company based in Dandong, China, with conspiring to evade U.S. economic sanctions and violating the Weapons of Mass Destruction Proliferators Sanctions Regulations (WMDPSR) through front companies by facilitating prohibited U.S. dollar transactions through the United States on behalf of a sanctioned entity in the Democratic People's Republic of Korea (North Korea) and to launder the proceeds of that criminal conduct through U.S. financial institutions. On Aug. 3, 2016, a U.S. Magistrate Judge in the District of New Jersey signed a criminal complaint charging Ma Xiaohong (Ma) and her company, Dandong Hongxiang Industrial Development Co. Ltd. (DHID), and three of DHID's top executives, general manager Zhou Jianshu (Zhou), deputy general manager Hong Jinhua (Hong) and financial manager Luo Chuanxu (Luo), with conspiracy to violate the International Emergency Economic Powers Act (IEEPA) and to defraud the United States; violating IEEPA; and conspiracy to launder monetary instruments. The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) also imposed sanctions on DHID, Ma, Zhou, Hong and Luo for their ties to the government of North Korea's weapons of mass destruction proliferation efforts. In addition, the department filed a civil forfeiture action for all funds contained in 25 Chinese bank accounts that allegedly belong to DHID and its front companies. The department has also requested that the federal court in the District of New Jersey issue a restraining order for all of the funds named in the civil forfeiture action, based upon the allegation that the funds represent property involved in money laundering, which makes them forfeitable to the United States. There are no allegations of wrongdoing by the U.S. correspondent banks or foreign banks that maintain these accounts. According to criminal and civil complaints, DHID is primarily owned by Ma and is located near the North Korean border. DHID allegedly openly worked with North Korea-based Korea Kwangson Banking Corporation (KKBC) prior to Aug. 11, 2009, when the OFAC designated KKBC as a Specially Designated National (SDN) for providing U.S. dollar financial services for two other North Korean entities, Tanchon Commercial Bank (Tanchon) and Korea Hyoksin

Trading Corporation (Hyoksin). President Bush identified Tanchon as a weapons of mass destruction proliferator in Jun. 2005, and OFAC designated Hyoksin as an SDN under the WMDPSR in Jul. 2009. Tanchon and Hyoksin were so identified and designated because of their ties to Korea Mining Development Trading Company (KOMID), which OFAC has described as North Korea's premier arms dealer and main exporter of goods and equipment related to ballistic missiles and conventional weapons. The United Nations (UN) placed KOMID, Tanchon and Hyoksin on the UN Sanctions List in 2006. In Mar. 2016, KKBC was added to the UN Sanctions List. In Aug. 2009, Ma allegedly conspired with Zhou, Hong and Luo to create or acquire numerous front companies to conduct U.S. dollar transactions designed to evade U.S. sanctions. The complaints allege that from Aug. 2009, to Sep. 2015, DHID used these front companies, established in offshore jurisdictions such as the British Virgin Islands, the Seychelles and Hong Kong, and opened Chinese bank accounts to conduct U.S. dollar financial transactions through the U.S. banking system when completing sales to North Korea. These sales transactions were allegedly financed or guaranteed by KKBC. These front companies facilitated the financial transactions to hide KKBC's presence from correspondent banks in the United States, according to the allegations in the complaints. As a result of the defendants' alleged scheme, KKBC was able to cause financial transactions in U.S. dollars to transit through the U.S. correspondent banks without being detected by the banks and, thus, were not blocked under the WMDPSR program. The case was investigated by the FBI.

***Systems and Components for Marine Submersible Vehicles to China*** – On Sept. 26, 2016, in the Middle District of Florida, Amin Yu was sentenced to 21 months in federal prison for acting in the U.S. as an illegal agent of a foreign government without prior notification to the Attorney General and for conspiring to commit international money laundering. According to the plea agreement dated Jun. 10, 2016, from at least 2002 until Feb. 2014, at the direction of co-conspirators working for Harbin Engineering University (HEU), a state-owned entity in the People's Republic of China, Yu obtained systems and components for marine submersible vehicles from companies in the United States. She then illegally exported those items to the PRC for use by her co-conspirators in the development of marine submersible vehicles – unmanned underwater vehicles, remotely operated vehicles and autonomous underwater vehicles – for HEU and other state-controlled entities. Yu illegally exported items by failing to file electronic export information (EEI), as required by U.S. law, and by filing false EEI. In particular, Yu completed and caused the completion of export-related documents in which she significantly undervalued the items that she had exported and provided false end user information for those items. Previously, on Apr. 21, 2016, an 18-count superseding indictment was unsealed in the Middle District of Florida charging Yu with acting as an illegal agent of a foreign government in the United States without prior notification to the Attorney General, conspiring to defraud the United States and to commit offenses against the United States, committing unlawful export information activities, smuggling goods from the United States, conspiring to and committing international money laundering and making false statements to the U.S. Citizenship and Immigration Services. This case was investigated by the FBI, U.S. Immigration and Customs Enforcement's Homeland Security Investigations, the Internal Revenue Service-Criminal Investigation and the Naval Criminal Investigative Service.

***Sensitive Technology to Pakistani Military*** – On Sept. 1, 2016, in the District of Arizona, Syed Vaqar Ashraf, of Lahore, Pakistan, was sentenced to 33 months in prison. Ashraf previously pleaded guilty to conspiracy to export defense controlled items without a license. Ashraf attempted to procure gyroscopes and illegally ship them to Pakistan so they could be used by the Pakistani military. In an effort to evade detection, Ashraf arranged for the gyroscopes to be purchased in the name of a shell company and caused the gyroscopes to be transshipped to Belgium. Ashraf then traveled to Belgium to inspect the gyroscopes and arrange for their final

transport to Pakistan. On Aug. 26, 2014, Ashraf was arrested by the Belgium Federal Police at the request of U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI) agents, who had been conducting an undercover investigation of Ashraf's activities. This case was investigated by ICE-HSI and Belgium Federal Police.

***Unmanned Aerial Vehicle to China*** – On Aug. 19, 2016, in the Southern District of Florida, Wenxia Man, aka Wency Man, was sentenced to 50 months in prison for conspiring to export and cause the export of fighter jet engines, an unmanned aerial vehicle – commonly known as a drone – and related technical data to the People's Republic of China in violation of the Arms Export Control Act. Previously, on Jun. 9, 2016, Man was convicted by a federal jury in the Southern District of Florida of one count of conspiring to export and cause the export of defense articles without the required license. According to evidence presented at trial, between approximately Mar. 2011, and Jun. 2013, Man conspired with Xinsheng Zhang, who was located in China, to illegally acquire and export to China defense articles including: Pratt & Whitney F135-PW-100 engines used in the F-35 Joint Strike Fighter; Pratt & Whitney F119-PW-100 turbofan engines used in the F-22 Raptor fighter jet; General Electric F110-GE-132 engines designed for the F-16 fighter jet; the General Atomics MQ-9 Reaper/Predator B Unmanned Aerial Vehicle, capable of firing Hellfire Missiles; and technical data for each of these defense articles. During the course of the investigation, when talking to an undercover HSI agent, Man referred to Zhang as a “technology spy” who worked on behalf of the Chinese military to copy items obtained from other countries and stated that he was particularly interested in stealth technology. This case was investigated by HSI and DCIS.

***Defense Articles to Sudan*** – On Aug. 4, 2016, in the Eastern District of Virginia, Elias Abdl Halim Ghandi, aka's Eliyas Ghandi, Elias Woldemariam, and Elias Ghandi Ahmed, a United States citizen, was sentenced to 40 months' imprisonment, two years' supervised release and \$100 special assessment following a plea of guilty on May 18, 2016, to violating the Arms Export Control Act. Ghandi pleaded guilty to a one-count information alleging that he knowingly and willfully attempted to export and exported rifles, pistols, and shotguns, which are defense articles on the U.S. Munitions List, from the United States to Khartoum, Sudan, without first obtaining the required license from the State Department. According to court documents, from May 6, 2012, to Nov. 20, 2014, Ghandi purchased twenty firearms from three firearms dealers on eighteen separate occasions and repeatedly traveled to Khartoum. Ghandi admitted that over the years, he had brought 20-30 guns into Sudan where he said that American guns were popular and sold well. The investigation was conducted by the U.S. Department of Homeland Security, Homeland Security Investigations.

***Sensitive Military and Export Controlled Data to China*** – On Jul. 13, 2016, in the Central District of California, Su Bin, also known as Stephen Su and Stephen Subin, a Chinese national and resident of the People's Republic of China, was sentenced to 46 months' imprisonment, a fine of \$10,000 and one year of supervised release. Previously, on Mar. 23, 2016, Su Bin pleaded guilty to participating in a years-long conspiracy to hack into the computer networks of major U.S. defense contractors, steal sensitive military and export-controlled data and send the stolen data to China. A criminal complaint filed in 2014 and subsequent indictments filed in Los Angeles charged Su Bin, a China-based businessman in the aviation and aerospace fields, for his role in the criminal conspiracy to steal military technical data, including data relating to the C-17 strategic transport aircraft and certain fighter jets produced for the U.S. military. Su was initially arrested in Canada in Jul. 2014, on a warrant issued in relation to this case. Su ultimately waived extradition and consented to be conveyed to the United States in Feb. 2016. In the plea agreement, Su admitted to conspiring with two persons in China from Oct. 2008, to Mar. 2014, to gain unauthorized access to protected computer networks in the United States, including

computers belonging to the Boeing Company in Orange County, California, to obtain sensitive military information and to export that information illegally from the United States to China. As part of the conspiracy, Su would e-mail the co-conspirators with guidance regarding what persons, companies and technologies to target during their computer intrusions. One of Su's co-conspirators would then gain access to information residing on computers of U.S. companies and email Su directory file listings and folders showing the data that the co-conspirator had been able to access. Su then directed his co-conspirator as to which files and folders his co-conspirator should steal. Once the co-conspirator stole the data, including by using techniques to avoid detection when hacking the victim computers, Su translated the contents of certain stolen data from English into Chinese. In addition, Su and his co-conspirators each wrote, revised and emailed reports about the information and technology they had acquired by their hacking activities, including its value, to the final beneficiaries of their hacking activities. Su's plea agreement makes clear that the information he and his co-conspirators intentionally stole included data listed on the U.S. Munitions List contained in the International Traffic in Arms Regulations. Su also admitted that he engaged in the crime for the purpose of financial gain and specifically sought to profit from selling the data the he and his co-conspirators illegally acquired. This case was investigated by the FBI, U.S. Air Force's Office of Special Investigations, OIA and NSD CES.

***Satellite Trade Secrets to Undercover Agent*** – On Jul. 7, 2016, in the Central District of California, Gregory Allen Justice was arrested by FBI special agents on federal charges of economic espionage and violations of the Arms Export Control Act for his attempts to sell sensitive satellite information to a person he believed to be a foreign intelligence agent. Justice worked for a cleared defense contractor as an engineer on military and commercial satellites during his alleged crimes. According to the affidavit in support of the criminal complaint, Justice stole proprietary trade secret materials from his employer and provided them to a person whom he believed to be a representative of a foreign intelligence service, but who was in fact an FBI undercover agent. In addition to their proprietary nature, the documents contained technical data covered by the U.S. Munitions List and therefore controlled for export from the United States under the International Traffic in Arms Regulations, according to the allegations. In exchange for providing these materials, Justice allegedly sought and received cash payments. This investigation was conducted by the FBI and AFOSI.

***High Tech U.S. Military Hardware to China*** – On Jun. 29, 2016, in the District of Delaware, Kan Chen of Ningbo, China, in Zhejiang Province, was sentenced to 30 months in prison and three years of supervised release for conspiring to violate the Arms Export Control Act and International Traffic in Arms Regulations; attempting to violate the Arms Export Control Act and International Traffic in Arms Regulations; and violating the International Emergency Economic Powers Act. On Jun. 16, 2015, Chen was arrested by HSI agents on the Northern Mariana Island of Saipan following an eight-month long investigation into his illegal conduct and has remained in custody. He pleaded guilty to the offenses listed above on Mar. 2, 2016. According to court documents, from Jul. 2013, through his arrest in Jun. 2015, Chen caused or attempted to cause the illegal export of over 180 export-controlled items, valued at over \$275,000, from the United States to China. Over 40 of those items – purchased for more than \$190,000 – were sophisticated night vision and thermal imaging scopes, which are designated by the International Traffic in Arms Regulations as U.S. Munitions List defense articles and can be mounted on automatic and semi-automatic rifles and used for military purposes at night. Given the sensitivity surrounding these military-grade items, Chen devised a scheme to smuggle these items through Delaware and outside the United States. He purchased the devices via the internet and telephone and had them mailed to several reshipping services in New Castle, Delaware, which provide an American shipping address for customers located in China, accept packages for their customers and then re-

shipped them to China. In order to further conceal his illegal activity, Chen arranged for the reshippers to send the devices to several intermediary individuals, who in turn forwarded the devices to Chen in China. Chen then sent the devices to his customers. During the course of this conduct, Chen made numerous false statements in order to knowingly and willfully evade the export control laws of the United States, including by undervaluing the shipments, unlawfully avoiding the filing of export information with the U.S. government, indicating that he was a natural-born U.S. citizen and providing the address of the reshipping service as his own. During the sentencing hearing, the government noted the lethality of these items when combined with weapons designed for use on a battlefield. For example, the ATN ThOR 640-5x, 640x480-Inch Thermal Weapon Scope, 100 mm, which Chen purchased for \$8,428.39, is described by the manufacturer as “an ideal product for force protection, border patrol officers, police SWAT and special operations forces providing them the tools they need to be successful in all field operations both day and night. Uncooled thermal imaging cuts through dust, smoke, fog, haze, and other battlefield obscurants.” These rifle scopes, therefore, are weapons of war, and Chen’s smuggling and subsequent sale of these military-grade items outside of the United States directly undermines our nation’s national security interests. As the government further noted, Chen’s conduct was particularly harmful because he sold this military technology indiscriminately. Thus, it could have ended up in any number of nefarious hands – including agents of foreign governments, bad actors and brokers. Once these rifle scopes were exported to China and distributed by Chen to his customers, the military technology contained inside these items could have been reversed engineered or used anywhere in the world for a variety of purposes by oppressive regimes, terrorists, or others to threaten the United States or its allies’ military advantage or to commit human rights abuses. This case was investigated by HSI and U.S. Department of Commerce-Bureau of Industry and Security’s Office of Export Enforcement.

***Theft of Trade Secrets*** – On Jun. 17, 2016, Dr. Lin Cheng, an American citizen, was sentenced in the Middle District of North Carolina to one year and one day of imprisonment, three years of supervised release, \$100 special assessment, and \$10,000 fine. Previously, on Dec. 9, 2015, Dr. Cheng pleaded guilty to possessing a stolen trade secret. Dr. Cheng was employed by Cree, Inc. from Nov. 2008, to Oct. 2014, as a Scientist. Specifically, Dr. Cheng was the engineering manager for Cree’s fourth generation of MOSFET technology. On Sep. 4, 2014, Cree informed the FBI that on Aug. 27, 2014, Dr. Cheng emailed a file containing Cree’s proprietary information from her work email at Cree to a Gmail account. The file contained the step-by-step process Cree uses to manufacture MOSFET technology. Cree determined that the proprietary and confidential files which were removed by Dr. Cheng from the control of Cree could cause both financial damage and technological loss to Cree. This case was investigated by FBI and Department of Energy, Office of Inspector General.

***High-Tech Material Used in Missile Production and Nuclear Applications to Iran*** – On Jun. 14, 2016, in the Eastern District of New York, Erdal Kuyumcu, the CEO of Global Metallurgy LLC, a company based in Woodside, New York, pleaded guilty to one count of conspiring to violate the International Emergency Economic Powers Act, in connection with the export of specialty metals from the United States to Iran. As detailed in the criminal information to which he pleaded guilty and other court filings, Kuyumcu, a U.S. citizen, conspired to export from the United States to Iran a metallic powder composed of cobalt and nickel, without having obtained the required license from the U.S. Treasury Department’s Office of Foreign Assets Control (OFAC). The metallic powder can be used to coat gas turbine components, including turbine blades, and can be used in aerospace, missile production and nuclear applications. Such specialized metals are closely regulated by the U.S. Department of Commerce to combat nuclear proliferation and protect national security, and exporting them without an OFAC license is illegal. Kuyumcu and others conspired to obtain over 1,000 pounds of the metallic powder from a U.S.-



based supplier for export to Iran. To hide the true destination of the goods from the U.S. supplier, Kuyumcu and a co-conspirator arranged for the metallic powder to be shipped first to Turkey and then to Iran. At sentencing, Kuyumcu faces up to 20 years in prison and a \$1 million fine. This case was investigated by the Commerce Department and the FBI.

***Theft of Valuable Source Code*** – On Jun. 14, 2016, Jiaqiang Xu was charged in the Southern District of New York in a six-count superseding indictment with economic espionage and theft of trade secrets, in connection with Xu’s theft of proprietary source code from his former employer, with the intent to benefit the National Health and Family Planning Commission of the People’s Republic of China. Xu was initially arrested by the FBI on Dec. 7, 2015, and subsequently charged on Jan. 6, 2016, by indictment with one count of theft of trade secrets. According to court documents, from Nov. 2010, to May 2014, Xu worked as a developer for a particular U.S. company (the “Victim Company”). As a developer, Xu enjoyed access to certain proprietary software (the “Proprietary Software”), as well as that software’s underlying source code (the “Proprietary Source Code”). The Proprietary Software is a clustered file system developed and marketed by the Victim Company in the U.S. and other countries. A clustered file system facilitates faster computer performance by coordinating work among multiple servers. The Victim Company takes significant precautions to protect the Proprietary Source Code as a trade secret. The Victim Company takes these precautions in part because the Proprietary Software and the Proprietary Source Code are economically valuable, which value depends in part on the Proprietary Source Code’s secrecy. In May 2014, Xu voluntarily resigned from the Victim Company. Xu subsequently, in a series of communication with UC agents, uploaded Victim Company’s Proprietary Source Code to the UC’s computer network. On Dec. 7, 2015, Xu met with UC-2 at a hotel in White Plains, New York (the Hotel). Xu stated, in sum and substance, that Xu had used the Proprietary Source Code to make software to sell to customers, that Xu knew the Proprietary Source Code to be the product of decades of work on the part of the Victim Company, and that Xu had used the Proprietary Source Code to build a copy of the Proprietary Software, which Xu had uploaded and installed on the UC Network (i.e., the Xu Upload). Xu also indicated that Xu knew the copy of the Proprietary Software that Xu had installed on the UC Network contained information identifying the Proprietary Software as the Victim Company’s property, which could reveal the fact that the Proprietary Software had been built with the Proprietary Source Code without the Victim Company’s authorization. Xu told UC-2 that Xu could take steps to prevent detection of the Proprietary Software’s origins – i.e., that it had been built with stolen Proprietary Source Code – including writing computer scripts that would modify the Proprietary Source Code to conceal its origins. Later on Dec. 7, 2015, Xu met with UC-1 and UC-2 at the Hotel. During that meeting, Xu showed UC-2 a copy of what Xu represented to be the Proprietary Source Code on Xu’s laptop. Xu noted to UC-2 a portion of the code that indicated it originated with the Victim Company as well as the date on which it had been copyrighted. Xu also stated that Xu had previously modified the Proprietary Source Code’s command interface to conceal the fact that the Proprietary Source Code originated with the Victim Company and identified multiple specific customers to whom Xu had previously provided the Proprietary Software using Xu’s stolen copy of the Proprietary Source Code. This case was investigated by the FBI.

***Tactical Equipment to Insurgent Groups in Syria*** – On Jun. 10, 2016, in the Eastern District of Virginia, Amin al-Baroudi, a Syrian-born naturalized U.S. citizen, formerly of Irvine, California, was sentenced to 32 months in prison for conspiring to export U.S.-origin goods from the United States to Syria, in violation of sanctions imposed on Syria by the U.S. government. Baroudi pleaded guilty on Jan. 15, 2016, to conspiracy to export U.S. goods to Syria, in violation of the International Emergency Economic Powers Act, 50 U.S.C. §§ 1702 and 1705(a) and (c). According to court documents, Baroudi admitted that from at least Dec. 2011, through Mar. 2013,

he and his co-conspirators exported U.S. tactical equipment to Syria for the purpose of supplying and arming Ahrar al-Sham and other insurgent groups in Syria whose stated goal is to overthrow the Assad government and install an Islamic state. Ahrar al-Sham frequently fights alongside Jabhat al-Nusra, which has been designated by the U.S. State Department as a foreign terrorist organization and operates as al-Qaeda's official branch in Syria. According to court documents, Baroudi and his co-conspirators purchased tens of thousands of dollars-worth of goods from companies and vendors in the United States, consisting largely of tactical equipment such as sniper rifle scopes, night vision rifle scopes, night vision goggles, laser bore sighters, speed loaders and bullet proof vests. Baroudi and his co-conspirators traveled with the goods aboard commercial flights to Turkey and then transported the goods into Syria or provided them to others for transport. Baroudi made two such trips in Feb. and Mar. of 2013. This case was investigated by the FBI, DOC OEE, ICE HSI, California Highway Patrol; the Irvine Police Department; the Orange County, California, Sheriff's Department; and the Regional Computer Forensics Laboratory in Orange County provided significant assistance.

***High-Grade Carbon Fiber to China*** – On Jun. 9, 2016, Fuyi Sun, a/k/a “Frank”, a citizen of the People's Republic of China, was charged in a one count indictment in the Southern District of New York with attempt to violate the International Emergency Economic Powers Act (“IEEPA”). Previously, on Apr. 13, 2016, Sun was arrested in connection with a scheme to illegally export to China, without a license, high-grade carbon fiber that is used primarily in aerospace and military applications. Sun was arrested after traveling to New York to meet with undercover agents (UCs) in an effort to obtain the specialized fiber, which – due to its military and aerospace applications – requires an export license for export to China. Sun was originally charged on Apr. 13, 2016, by a three count Complaint which charged Sun with: Count One – attempt to violate the International Emergency Economic Powers Act (“IEEPA”); Count Two – conspiracy to violate IEEPA; and Count Three – attempt to smuggle goods from the United States. According to Court documents, Sun attempted for years to acquire high-grade carbon fiber for illegal export to China. After traveling to New York from China to finalize the deal, Sun allegedly told the UCs that the carbon fiber he sought was headed to the Chinese military. He then paid tens of thousands of dollars in cash to purchase two cases of it. To avoid law enforcement detection, Sun allegedly directed the UCs to ship the carbon fiber in unmarked boxes and to falsify the shipping documents regarding the contents of the boxes. Courts documents also state that, since approximately 2011, Sun has attempted to acquire extremely high-grade carbon fiber, including Toray type M60JB-3000-50B carbon fiber (“M60 Carbon Fiber”). M60 Carbon Fiber has applications in aerospace technologies, unmanned aerial vehicles (commonly known as “drones”) and other government defense applications. Accordingly, M60 Carbon Fiber is strictly controlled – including that it requires a license for export to China – for nuclear non-proliferation and anti-terrorism reasons. In furtherance of his attempts to illegally export M60 Carbon Fiber from the United States to China without a license, Sun contacted what he believed was a distributor of carbon fiber – but which was, in fact, an undercover entity created by HSI and “staffed” by HSI UCs. Sun inquired about purchasing the M60 Carbon Fiber without the required license. In the course of his years-long communications with the UCs and the UC Company, Sun repeatedly suggested various security measures that he believed would protect them from “U.S. intelligence.” Among other such measures, at one point, Sun instructed the UCs to use the term “banana” instead of “carbon fiber” in their communications. Consequently, soon thereafter he inquired about purchasing 450 kilograms of “banana” for more than \$62,000. In order to avoid detection, Sun also suggested removing the identifying barcodes for the M60 Carbon Fiber, prior to transshipment, and further suggested that they identify the M60 Carbon Fiber as “acrylic fiber” in customs documents. On or about Apr. 11, 2016, Sun traveled from China to New York for the purpose of purchasing M60 Carbon Fiber from the UC Company. During meetings with the UCs, on or about Apr. 11 and 12, 2016, among other things, Sun repeatedly suggested that the Chinese military was the

ultimate end-user for the M60 Carbon Fiber he sought to acquire from the UC Company. Sun claimed to have personally worked in the Chinese missile program. Sun also asserted that he maintained a close relationship with the Chinese military, had a sophisticated understanding of the Chinese military's need for carbon fiber, and suggested that he would be supplying the M60 Carbon Fiber to the Chinese military or to institutions closely associated with it. On or about Apr. 12, 2016, Sun agreed to purchase two cases of M60 Carbon Fiber from the UC Company. Sun paid the UCs \$23,000 in cash for the carbon fiber. He also paid an additional \$2,000 to the UCs as compensation for the risk he believed they were taking to illegally export the carbon fiber to China without a license. This investigation was conducted by DOC, HSI, and DCIS.

***High-Tech Electronic Components to Iran*** – On May 23, 2016, in the Southern District of New York, Ali Reza Parsa, a Canadian-Iranian dual citizen and resident of Canada, was sentenced to three years in prison for his participation in a conspiracy to violate the International Emergency Economic Powers Act (IEEPA) and the Iranian Transactions and Sanctions Regulations (ITSR). Parsa was arrested in Oct. 2014, following an investigation by the FBI and U.S. Department of Commerce's Bureau of Industry and Security (BIS). He pleaded guilty on Jan. 20, 2016. According to court documents, between approximately 2009 and 2015, Parsa conspired to obtain high-tech electronic components from American companies for transshipment to Iran and other countries for clients of Parsa's procurement company in Iran, Tavan Payesh Mad, in violation of U.S. economic sanctions. To accomplish this, Parsa used his Canadian company, Metal PM, to place orders with U.S. suppliers and typically had the parts shipped to him in Canada or to a freight forwarder located in the United Arab Emirates, and then shipped from these locations to Iran or to the location of his Iranian company's client. Parsa provided the U.S. companies with false destination and end-user information about the components in order to conceal the illegality of these transactions. Parsa's criminal scheme targeted numerous American technology companies. The components that Parsa attempted to procure included cryogenic accelerometers, which are sensitive components that measure acceleration at very low temperatures. Cryogenic accelerators have both commercial and military uses, including in applications related to ballistic missile propellants and in aerospace components such as liquid-fuel rocket engines. In addition, following his arrest and while incarcerated, Parsa continued to violate the IEEPA and the ITSR by conducting business for Metal PM and Tavan Payesh Mad, including by ordering parts from German and Brazilian companies for Iranian customers. Parsa subsequently directed a relative to delete email evidence of his ongoing business transactions while in jail and emphasized the need for secrecy in their dealings. Neither Parsa nor any other individual or entity involved in transactions that gave rise to his conviction applied for or obtained a license from the U.S. Department of the Treasury's Office of Foreign Assets Control for the transactions. This case was investigated by the FBI and Department of Commerce BIS.

***Defense Materials to India*** – On Apr. 14, 2016, in the District of New Jersey, Hannah Robert, the owner of two New Jersey defense contracting businesses, was sentenced to 57 months in prison for conspiring to send sensitive military technical data to India. Previously, on Apr. 1, 2015, Robert pleaded guilty to one count of conspiracy to violate the Arms Export Control Act (22 U.S.C. § 2778). On Oct. 28, 2013, Robert was arraigned for allegedly transmitting military technical drawings to India without first obtaining a license from the U.S. Department of State, in violation of U.S. export laws. She was indicted by a federal grand jury on Oct. 10, 2013, on one count of violating the Arms Export Control Act and one count of conspiracy to violate the act. According to the documents filed in this case and statements made in court, Robert was the founder, owner, and President of One Source USA LLC, a company located at her then-residence in Mount Laurel, N.J., and contracted with the U.S. Department of Defense (DoD) to supply defense hardware items and spare parts pursuant to government contracts. In Sep. 2012, Robert opened a second defense-contracting company, Caldwell Components Inc., based at the same

address in Mount Laurel. Along with "R.P.," a resident of India, Robert owned and operated a company in India, One Source (One Source India), that manufactured defense hardware items and spare parts in India. From Jun. 2010 to Dec. 2012, Robert and R.P. conspired to export to India defense technical drawings without obtaining the necessary licenses from the U.S. Department of State. The exported technical drawings include parts used in the torpedo systems for nuclear submarines, in military attack helicopters, and in F-15 fighter aircraft. Robert allegedly lied on her bids for DoD contracts, stating that she would be supplying American-made products and that her N.J.-based company was a manufacturer, rather than a dealer, of defense spare parts. One Source USA also subcontracted to other American defense contractors, including those in Sussex County, N.J., and Boca Raton, Fla. Robert provided export-controlled items made in India to these defense contractors in the United States in such a way as to appear to the DoD that the items were manufactured in this country. In addition to United States' sales, Robert and R.P. sold defense hardware items to foreign customers. Robert transmitted export-controlled technical data to R.P. in India so that Robert and R.P. could submit bids to foreign actors, including those in the United Arab Emirates (UAE), to supply them or their foreign customers with defense hardware items and spare parts. Neither Robert nor R.P. obtained approval from the U.S. Department of State for this conduct. On Aug. 23, 2012, R.P. e-mailed Robert from India requesting the technical drawing for a particular military item. R.P.'s e-mail forwarded Robert an e-mail from an individual purporting to be "an official contractor of the UAE Ministry of Defence," and who listed a business address in Abu Dhabi, UAE. The UAE e-mail requested quotations for a bid for the "blanket assembly" for the CH-47F Chinook military helicopter and listed the "End User" for the hardware item as the UAE Armed Forces. Later that same day, Robert replied to R.P.'s e-mail, attaching, among other things, the electronic file for an export-controlled technical drawing titled "Installation and Assy Acoustic Blankets, STA 120 CH-47F," to be used in the Chinook attack helicopter. Starting in Oct. 2010, Robert transmitted the military drawings for these parts to India by posting the technical data to the password-protected website of a Camden County, N.J., church where she was a volunteer web administrator. This was done without the knowledge of the church staff. Robert e-mailed R.P. the username and password to the church website so that R.P. could download the files from India. Through the course of the scheme, Robert uploaded thousands of technical drawings to the church website for R.P. to download in India. On Jun. 25, 2012, R.P. e-mailed Robert from India, stating in part: "Please send me the church web site username and password." The e-mail was in reference to both an invoice to, and a quote for, an individual known to Robert as a broker of defense hardware items for an end-user in Pakistan. This individual (the "Pakistan trans-shipper") employed a UAE address for shipping purposes. This case was investigated by DoD, DCIS, and DHS HSI Counter Proliferation Investigations.

***F-14 Fighter Jet Parts to Iran*** – On Apr. 5, 2016, in the Northern District of Georgia, Oguzhan Aydin was sentenced to 30 months' imprisonment, 5 years supervised release, \$200 special assessment and a \$25,000 fine. Aydin pleaded guilty on Oct. 13, 2015, to exporting munitions out of the United States and money laundering. Previously, on Aug. 26, 2014, Aydin was arrested pursuant to an arrest warrant in the Northern District of Georgia. A federal grand jury returned an indictment charging Aydin, Saeid Kamyari, AGM Ltd. Co. and Blue Sky Aviation with violations of the Arms Export Control Act and the International Emergency Economic Powers Act. According to court documents, between Sep. 2009, and Aug. 2010, Kamyari, while in Iran, worked through AGM Ltd. Co., a company located in Tehran, Iran, to procure aircraft parts for the F-14 Fighter Jet and other aircraft parts for shipment from the U.S. to Iran. Aydin, while in the Republic of Turkey, assisted Kamyari through his association with Blue Sky Aviation a.k.a. BSA Hava Kargo Ltd. Sti. Using e-mails, Kamyari and Aydin coordinated and arranged through AGM LTD Co. and Blue Sky Aviation, the purchase and export of microcircuits designed for use on F-14 fighter jets and other aircraft parts for shipment from the

U.S. through Turkey to Iran. At no time did the co-conspirators obtain a license to export aircraft parts from the U.S. to Iran. This investigation was conducted by DHS.

***Sanctions Violations to Aid the Government of Iran*** – On Mar. 21, 2016, an indictment was unsealed in the Southern District of New York against Reza Zarrab, aka Riza Sarraf, a resident of Turkey and dual citizen of Turkey and Iran; Camelia Jamshidy, aka Kamelia Jamshidy, a citizen of Iran; and Hossein Najafzadeh, a citizen of Iran, for engaging in hundreds of millions of dollars-worth of transactions on behalf of the government of Iran and other Iranian entities, which were barred by U.S. sanctions, laundering the proceeds of those illegal transactions and defrauding several financial institutions by concealing the true nature of these transactions. Zarrab was arrested on Mar. 19, 2016, and had his initial court appearance in Miami, Florida, on Mar. 21, 2016. Jamshidy and Najafzadeh remain at large. According to the allegations contained in the indictment, between 2010 and 2015, Zarrab, Jamshidy and Najafzadeh conspired to conduct international financial transactions on behalf of and for the benefit of, among others, Iranian businesses, the Iranian government and entities owned or controlled by the Iranian government. Among the beneficiaries of these schemes were: Bank Mellat, an Iranian government-owned bank designated, during the time of the charged offenses, by the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) as a Specially Designated National (SDN) under the Iranian Transactions and Sanctions Regulations, the Iranian Financial Sanctions Regulations and the Weapons of Mass Destruction Proliferators Sanctions Regulations; Mellat Exchange, an Iranian money services business owned and controlled by Bank Mellat; the National Iranian Oil Company (NIOC), identified during the time of the charged offenses by OFAC as an agent or affiliate of Iran’s Islamic Revolutionary Guard Corp (IRGC); the Naftiran Intertrade Company Ltd. (NICO), Naftiran Intertrade Company Sarl (NICO Sarl) and Hong Kong Intertrade Company (KHICO), companies located in the United Kingdom, Switzerland and Hong Kong, respectively, that were acting on behalf of NIOC; and the MAPNA Group, an Iranian construction and power plant company. Bank Mellat, NIOC, NICO Sarl, NICO and KHICO are no longer designated as SDNs and NIOC is no longer identified as an agent or affiliate of the IRGC, though these entities remain “blocked parties,” with whom U.S. persons continue to be prohibited generally from engaging in unlicensed transactions or dealings. The scheme was part of an intentional effort to assist the government of Iran in evading the effects of United States and international economic sanctions. Zarrab, Jamshidy, Najafzadeh and their co-conspirators used an international network of companies located in Iran, Turkey and elsewhere to conceal from U.S. banks, OFAC and others that the transactions were on behalf of and for the benefit of Iranian entities. This network of companies includes Royal Holding A.S., a holding company in Turkey; Durak Doviz Exchange, a money services business in Turkey; Al Nafees Exchange, a money services business; Royal Emerald Investments; Asi Kiyemetli Madenler Turizm Otom, a company located in Turkey; ECB Kuyumculuk Ic Vedis Sanayi Ticaret Limited Sirketi, a company located in Turkey; and Gunes General Trading LLC; and others. As a result of this scheme, the co-conspirators induced U.S. banks to unknowingly process international financial transactions in violation of the IEEPA. The case was investigated by the FBI.

***Technology Equipment to China*** – On Mar. 2, 2016, Louis Brothers was sentenced in the Eastern District of Kentucky to 93 months in prison for illegally exporting sophisticated technology equipment to the People’s Republic of China (PRC) and concealing the unlawful proceeds. The sentence also includes a monetary judgment of \$1.1 million. Brothers, a former president and CEO of Valley Forge Composite Technologies, pleaded guilty to the offenses in Jul. 2015. He admitted that from 2009 until 2013, he unlawfully exported microcircuits to the PRC. Under federal law, anyone exporting a defense article, including microcircuits, to the PRC must obtain the permission of the Department of State for the purposes of maintaining national

security. According to his plea agreement, Brothers intentionally avoided notifying the Department of State about his activity and labeled his shipments as “computer parts” in order to conceal the true identity of the items. Brothers further admitted that he falsified paperwork to make it appear that the proceeds he received from his business with the PRC were actually profits from a business he owned in Kentucky. The investigation was conducted by the FBI and ICE HSI.

***Night Vision Devices to China*** – On Feb. 29, 2016, Song Il Kim, aka Kim Song Il was sentenced in the District of Utah to 40 months’ imprisonment, 36 months supervised release and \$100 special assessment after pleading guilty on Dec. 9, 2015, to violating the Arms Export Control Act. Kim attempted to export from the United States to China night vision devices without first obtaining a license from the State Department.

***Pressure Transducers to Iran*** – On Jan. 27, 2016, Sihai Cheng, a citizen of the People’s Republic of China (PRC), was sentenced in the District of Massachusetts to nine years imprisonment and \$600 special assessment after pleading guilty on Dec. 18, 2015, to two counts of conspiring to commit export violations and smuggle goods from the U.S. to Iran and four counts of illegally exporting U.S. manufactured pressure transducers to Iran. In Feb. 2014, Cheng was arrested by the British authorities on U.S. charges during a trip to the United Kingdom. He was detained in the United Kingdom pending extradition to the United States. Cheng arrived in Boston from the United Kingdom on Dec. 5, 2014. On Apr. 4, 2014, following an international investigation, Cheng and co-defendant Seyed Abolfazl Shahab Jamili, an Iranian national, were indicted along with two Iranian companies, Nicaro Eng. Co. and Eyvaz Technic Manufacturing Co., for conspiring to export American-made pressure transducers to Iran. Pressure transducers can be used in gas centrifuges to enrich uranium and produce weapons-grade uranium. The indictment alleged that between Nov. 2005 and 2012, Cheng supplied thousands of parts that have nuclear applications, including U.S.-origin goods, to Eyvaz, an Iranian company involved in the development and procurement of parts for Iran’s nuclear weapons program. In 2011, the Council of the European Union designated Eyvaz as an entity “involved in [Iran’s] nuclear or ballistic missile activities” and imposed restrictive measures against it. In so doing, it found that Eyvaz had produced vacuum equipment, which it supplied to two of Iran’s uranium nuclear enrichment facilities, Natanz and Fordow, and that it also had supplied pressure transducers to Kalaye Electric Company, an Iranian company which has been designated by the U.S. and United Nations as a proliferator of Weapons of Mass Destruction. Specifically, the indictment alleged that in 2005, Cheng began doing business with Jamili, who worked for Eyvaz and ran his own importing business in Iran. Beginning in Feb. 2009, Cheng and Jamili conspired with others in the PRC to illegally obtain hundreds of U.S. manufactured pressure transducers manufactured by MKS Instruments, Inc., headquartered in Massachusetts, on behalf of Eyvaz. As a result of the illegal activities of Cheng and his co-conspirators, hundreds of MKS pressure transducers were illegally exported from the U.S. to China. Upon receipt of these parts in China, Cheng caused the MKS pressure transducers to be exported to Eyvaz or Jamili in Tehran, Iran, in violation of U.S. export laws. The indictment further alleged that by 2007, Iran was operating thousands of gas centrifuges at the Natanz uranium enrichment facility. Iran has sought and illicitly obtained MKS pressure transducers to use in its centrifuge plants. Publicly available photographs of Natanz (with then President Mahmoud Ahmadinejad) show numerous MKS pressure transducers attached to Iran’s gas centrifuge cascades. Because pressure transducers can be used in gas centrifuges to convert natural uranium into a form that can be used in nuclear weapons, they are subject to export controls and cannot be shipped to China without an export license or to Iran at all. On Jan. 16, 2016, the indictment was dismissed against Jamili. This case was investigated by the FBI, U.S. Immigration and Customs Enforcement’s (ICE) Homeland Security Investigations (HSI) and the Department of Commerce’s Office of Export Enforcement.

***Military Aircraft Components to UAE, Thailand*** – On Jan. 15, 2016, John Nakkashian was sentenced in the Central District of California to 2 years’ probation, \$100 special assessment, and a fine of \$1,000 after previously pleading guilty on Aug. 28, 2014, to a 1st Superseding Information. Nakkashian admitted that he knowingly made a false statement on a Shipper’s Export Declaration Form that a military gyroscope being shipped to Thailand did not require an export license, when in fact it did. Nakkashian was a Vice President for International Sales at Air Shunt Instruments, Inc. Air Shunt, a Chatsworth, California company that buys and sells aircraft and aerospace components, was charged via criminal information and pleaded guilty in the Central District of California on Jul. 15, 2008. The company was sentenced on Jul. 17, 2008, and ordered to pay a criminal fine of \$250,000 and a special assessment of \$400 for making false statements on a Shipper’s Export Declaration in claiming that a military gyroscope being sent overseas in 2003 did not require an export license, when in fact the item required such a license. Nakkashian was responsible for obtaining the required licenses for such exports. On May 20, 2008, Nakkashian was indicted on four counts of violating the Arms Export Control Act. The indictment alleged that Nakkashian illegally exported components for the J85 engine used on the F-5 fighter jet, and other military items to Dubai, United Arab Emirates, without first obtaining the required export license from the State Department. The indictment also alleged that Nakkashian illegally exported a military gyroscope to Thailand. Nakkashian was arrested on Jun. 16, 2014, after fleeing the country during the investigation. The investigation was conducted by DCIS and ICE.

***Military Technical Drawings Downloaded/Exported Outside of the U.S.*** – On Dec. 8, 2015, in the District of New Jersey, Alper Calik of Ankara, Turkey and the former owner of two New Jersey defense contracting businesses was sentenced to time served, Special Assessment of \$100, and Restitution in the amount of \$347,240, after pleading guilty on Aug. 27, 2015, to a one-count Information charging him with committing mail fraud. Previously, on Sep. 13, 2014, Calik was arrested upon his entry into the United States. Calik was charged by complaint with two counts of mail fraud in connection with allegedly fraudulent contracts entered into with the U.S. Department of Defense (DoD), and one count of violating the Arms Export Control Act, in connection with his download of thousands of military technical drawings while outside the United States without prior approval from the U.S. Department of State. According to the complaint, starting in Nov. 2009, Calik was the co-owner of Clifmax LLC in Clifton, New Jersey. The company contracted with DoD to supply defense hardware items and spare parts. Starting in May 2011, Calik started a second defense-contracting company, Tunamann LLC, based at the same address in Clifton. Both Clifmax and Tunamann were allegedly “shell” companies for manufacturing facilities in Turkey, created to obtain DoD contracts that the manufacturers were not permitted to receive. Calik, on numerous occasions, falsely claimed to the DoD that Clifmax and Tunamann were U.S.-based manufacturers, when, in fact, neither company ever had any manufacturing capabilities in the United States. Calik is charged with violating the Arms Export Control Act. For both Clifmax and Tunamann, Calik submitted Military Critical Technical Data Agreements in which he claimed his companies were U.S.-based manufacturers. Calik also acknowledged that he understood export control laws and agreed not to disseminate export-controlled data and technical drawings in a manner that would violate export control laws. Based on his false representations, Calik was granted electronic access to drawings and technical data subject to U.S. export control regulations. Beginning in 2009, Calik downloaded approximately one hundred thousand drawings, some of which were subject to U.S. export control regulations. Calik was not in the United States when the majority of the drawings were downloaded and he did not obtain export licenses from the U.S. Department of State. On May 23, 2013, Calik, who at that time was operating Tunamann, downloaded from a DoD database the technical drawings for parts that go into the NSSN Class Submarine. Those drawings contained warnings stating that the

export of the drawings to places outside the United States is restricted by the Arms Export Control Act. Calik was not in the United States when those drawings were downloaded and he did not obtain an export license from the U.S. Department of State for the export of those drawings. This case was investigated by the Department of Defense, Defense Criminal Investigative Service and HSI, Counter Proliferation Investigations.

***Sniper Rifles to Belarus*** – On Dec. 2, 2015, in the District of Utah, a federal grand jury returned an indictment charging Kolar Rahman Anees Ur Rahman, age 44, who was born in India and lives in the United Arab Emirates, with violations of federal law in connection with alleged efforts to purchase 89 Sako .308 caliber sniper rifles and have them exported from the United States to Belarus. The charges in the four-count indictment include conspiracy to commit an offense against the United States, a violation of the Arms Export Control Act, smuggling goods from the United States, and money laundering. Rahman was arrested in early Nov. 2016, in Chicago on a complaint filed in Utah. Following a removal proceeding in Chicago, he was transferred to Salt Lake City by the U.S. Marshals Service. According to the indictment, it is the policy of the United States to deny licenses and other approvals for the export of defense articles and defense services destined for Belarus, as well as other countries subject to an arms embargo. According to the indictment, in Nov. 2013, a firearms manufacturer in Salt Lake City was contacted through email by someone identified as Individual A in the indictment regarding the purchase of 50 sniper rifles to be shipped to Belarus. The firearms manufacturer notified Individual A that the purchase and delivery would be impossible due to current trade sanctions and embargoes against Belarus. The firearms manufacturer subsequently informed a special agent with U.S. Immigration and Customs Enforcement’s Homeland Security Investigations (HSI) about the suspicious inquiry. An HSI Salt Lake City undercover agent contacted Individual A by email. In those communications, Individual A reiterated his desire to procure sniper rifles in the United States for delivery to Belarus. From Nov. 2013, through May 2015, negotiations between the undercover agent and Individual A did not result in a purchase. However, in May 2015, Individual A introduced the undercover agent to Rahman, designating Rahman as the principal broker for the procurement of the sniper rifles. The indictment alleged that from May 2015, until Nov. 2015, the defendant engaged in a conspiracy to purchase 89 sniper rifles in the United States and have them exported to Belarus without first obtaining licenses as required. In Aug. 2015, Rahman and an undercover agent agreed that Rahman would make a first purchase of 10 sniper rifles and ammunition for approximately \$66,285. No party to the transaction obtained export licenses for the rifles. In Sep. 2015, according to the indictment, Rahman informed the undercover agent that the final contract with Belarus had been completed and sent the undercover agent a down payment of approximately \$13,257 for 10 sniper rifles. Rahman agreed to pay the remaining balance once the rifles arrived in Belarus. He told the undercover agent not to include U.S. invoices with the shipment. Rahman requested that the sniper rifles be shipped by the most direct route possible to Belarus. According to the indictment, the undercover agent informed Rahman that the shipment route would be from the United States to South Africa, to Turkey and then to Belarus. On Nov. 4, 2015, two undercover HSI agents met with an individual who identified himself as Kolar Rahman Anees Ur Rahman at a hotel near Chicago, according to the indictment. Rahman confirmed he was the same individual the agents had been negotiating with since May. Rahman, the indictment alleged, informed the agents that he understood the risk of illegally obtaining and shipping the sniper rifles to Belarus and that he desired to complete their business transaction as planned. Rahman and the agents discussed future purchases and shipments of the .308 caliber rifles to Belarus. Rahman was arrested by the agents in Chicago later that day.

***Theft of Military Trade Secrets to Iran*** – On Oct. 27, 2015, Mozaffar Khazaee, also known as “Arash Khazaie”, was sentenced in the District of Connecticut to 97 months’ imprisonment, 3



years supervised release, \$100 special assessment and \$50,000 fine. Previously, on Feb. 25, 2015, Khazaei pleaded guilty to a one-count information charging him with unlawful export and attempted export of defense articles from the United States, in violation of the Arms Export Control Act. On Jan. 21, 2014, a federal grand jury returned an indictment charging Khazaei with two counts of interstate transportation of stolen property. The indictment stems from Khazaei's alleged attempt to ship to Iran proprietary material relating to military jet engines and the U.S. Air Force's F35 Joint Strike Fighter program that he had illegally retained from defense contractors where he had been employed. As alleged in court documents, federal law enforcement agents began investigating Khazaei in Nov. 2013, when officers with U.S. Customs and Border Protection Service (CBP), assisted by Homeland Security Investigations (HSI) special agents, inspected a shipment that Khazaei sent by truck from Connecticut to a freight forwarder located in Long Beach, California, which was intended for shipment from the U.S. to Iran. The documentation for Khazaei's shipment indicated that it contained household goods. Upon inspecting the shipment, however, CBP officers and HSI agents discovered that the content of the shipment primarily contained numerous boxes of documents consisting of sensitive technical manuals, specification sheets, and other proprietary material relating to the U.S. Air Force's F35 Joint Strike Fighter program and military jet engines. Upon further investigation, law enforcement learned that Khazaei holds Iranian and U.S. citizenship and, as recently as Aug. 2013, worked as an engineer for defense contractors, including firms that are the actual owners of the technical and proprietary documents and materials in Khazaei's shipment. Khazaei, who became a naturalized U.S. citizen in 1991, holds a valid U.S. passport. On Jan. 9, 2014, Khazaei was arrested by HSI and FBI agents at Newark Liberty International Airport in New Jersey after flying from Indianapolis to Newark, before he was able to board a connecting flight to Frankfurt, Germany. Khazaei's ticketed destination was Tehran, Iran. This case was investigated by HSI, CBP, the U.S. Air Force's Office of Special Investigations, DCIS, and the FBI.

***Schematics of the Navy's Nuclear Aircraft Carrier to Egypt*** – On Oct. 15, 2015, Navy Engineer Mostafa Ahmed Awwad was sentenced in the Eastern District of Virginia to 11 years of incarceration after having earlier plead guilty to attempted espionage. Awwad was originally arrested on Dec. 5, 2014, on charges of attempting to steal schematics of the Navy's newest nuclear aircraft carrier, the USS Gerald R. Ford, and pass the schematics to whom he believed was an Egyptian government official. Awwad was indicted on Dec. 3, 2014, and charged with two counts of attempted exportation of defense articles and technical data. According to court documents, Awwad began working for the Department of the Navy in Feb. 2014, as a civilian general engineer in the Nuclear Engineering and Planning Department at Norfolk Naval Shipyard. Based on a joint investigation, an FBI undercover agent speaking in Arabic contacted Awwad by telephone on Sep. 18, 2014, and asked to meet him the following day. Without seeking additional information from the caller, Awwad agreed. The next day Awwad met with the undercover FBI agent, who was posing as an Egyptian intelligence officer, in a park in Hampton, VA. During the meeting, Awwad claimed it was his intention to utilize his position of trust with the U.S. Navy to obtain military technology for use by the Egyptian government, including but not limited to, the designs of the USS Gerald R. Ford nuclear aircraft carrier. Awwad agreed to conduct clandestine communications with the undercover FBI agent by email and unattributable telephones and to conduct "dead drops" in a concealed location in the park. On Oct. 9, 2014, Awwad and the undercover FBI agent met at a hotel where Awwad described a detailed plan to circumvent U.S. Navy computer security by installing software on his restricted computer system that would enable him to copy documents without causing a security alert. At this time Awwad also provided the undercover FBI agent four Computer Aided Drawings of a U.S. nuclear aircraft carrier downloaded from the Navy Nuclear Propulsion Information system. These drawings were marked with warnings that foreign distribution could result in criminal prosecution. During the discussion, Awwad indicated his understanding that the drawings would be sent to and used in

Egypt. Awwad also asked the undercover FBI agent for \$1,500 to purchase a pinhole camera he would wear around the shipyard to photograph restricted material. At the conclusion of the meeting, Awwad agreed to provide the undercover FBI agent with passport photos which would be used to produce a fraudulent Egyptian passport so Awwad could travel to Egypt without alerting U.S. government officials. On Oct. 23, 2014, Awwad traveled to the pre-arranged dead drop site situated on a secluded hiking trail, and utilized a concealed container disguised in a hole in the ground. He retrieved \$3,000 in cash before placing a one terabyte external hard drive and two passport photos inside. The FBI later collected the contents of the dead drop container. On Nov. 28, 2014, Awwad was observed entering his office at the Norfolk Naval Shipyard holding a cardboard tube about three feet long. Once in his office, Awwad opened the cardboard tube and took out several white sheets which appeared to be design schematics of an aircraft carrier. Awwad then placed the schematics on the floor of his office and photographed them. After approximately 45 minutes of viewing the schematics and taking photographs, Awwad placed all the schematics back in the cardboard tube and left his office. Awwad plead guilty to the espionage charge on Jun. 15, 2015. This case was investigated by the FBI's Norfolk Field Office and the Naval Criminal Investigative Service, in cooperation with the Department of Navy.

***Gyroscope to Iran*** – On Aug. 27, 2015, Ali Mohammadi, a United States citizen, was sentenced in the Northern District of Illinois to 5 years' probation, a \$2,000 fine and \$100 special assessment. Previously, on Feb. 26, 2015, Mohammadi pleaded guilty to conspiracy to violate the International Emergency Economic Powers Act (IEEPA) and the U.S. sanctions against Iran. Mohammadi was the sole owner and operator of Modir Trading, an export business. According to court documents, Mohammadi, Modir Trading, and Ebrahim Hallaji, an Iranian national, conspired to export one Series 446 Rate Integrating Gyroscope, a component of the TOW missile, from the United States to Iran. Hallaji contacted Mohammadi by email in Feb. 2010, requesting that Mohammadi obtain certain gyroscope models to sell and export to Iran for Hallaji, who claimed to conduct import and export business in the United Arab Emirates. Hallaji informed Mohammadi that the items were prohibited to be sold directly to Iran. Mohammadi contacted a salesperson for gyroscopes and was told that he would need an export license to export the gyroscope internationally. The salesperson was an undercover agent. Mohammadi falsely informed the agent that the gyroscopes would be used as models in California. Mohammadi, Modir Trading, and Hallaji were indicted on Jul. 31, 2012. Hallaji remains a fugitive.

***Sensitive U.S. Technology to Iran*** – On Aug. 27, 2015, Arash Ghahreman, a naturalized U.S. citizen and former Iranian national, was sentenced in the Southern District of California to 78 months' imprisonment, 3 years supervised release, and \$100 special assessment. Previously, on Apr. 23, 2015, a federal jury convicted Ghahreman of violations of U.S. export and money laundering laws, arising from his involvement in a scheme to purchase marine navigation equipment and military electronic equipment for illegal export to, and end-use in, Iran. Ghahreman was convicted of attempted export to Iran, and conspiracy to do the same, in violation of the Iran Transactions and Sanctions Regulations; smuggling goods from the U.S., and conspiracy to do the same; and aiding and abetting the transfer of money from Dubai, United Arab Emirates (UAE), to the U.S., in support of an illegal export activity, and conspiracy to do the same. After a seven-day jury trial, the jury returned a guilty verdict on seven counts of a nine-count superseding indictment after only one day of deliberation. The jury was unable to reach a verdict on two of the counts involving the attempted exportation and smuggling of a fiber optic gyrocompass, used in both military and civilian marine navigation applications. The evidence presented at trial showed that Ghahreman acted as an agent of an Iranian procurement network which used a front company in Dubai to acquire U.S. goods and technologies for illegal transshipment to, and end-use in, Iran. Co-defendant Koorush Taherkhani, an Iranian national and resident, was the managing director and founder of that front company, co-defendant TIG

Marine Engineering Services. Because of his German nationality, co-defendant Ergun Yildiz, 35, a resident of UAE, was hired by Taherkhani to be the “face” of the front company, as the president/CEO of TIG Marine. Before Ghahreman immigrated to the U.S. in 2007, Ghahreman and Taherkhani had been friends and dorm mates at an Iranian university, where each received a degree in marine engineering. Upon graduation, both Ghahreman and Taherkhani worked as engineers for various Iranian shipping companies, including the Islamic Republic of Iran Shipping Lines and its subsidiaries. After immigrating to the U.S., Ghahreman was employed by various shipyards in the U.S., and became a naturalized U.S. citizen. Because of his employment and citizenship status, Ghahreman was well placed to act as an agent of the illegal procurement network. From Dec. 2012, through Jun. 17, 2013, Ghahreman and his co-defendants negotiated via email, text, telephone and meetings with U.S. Immigration Customs and Enforcement’s Homeland Security Investigations (ICE-HSI) and the Defense Criminal Investigative Service (DCIS) undercover agents to purchase marine navigation components (fiber optic gyrocompasses), military electronic components (electron tubes) and other U.S. technology for illegal export to, and/or end-use in, Iran. The undercover agents were posing as brokers of U.S. goods and technology, willing to sell U.S. goods to the defendants for end-use in Iran. Ultimately, as a result of these negotiations, Ghahreman and his co-defendants agreed to purchase four Navigat-2100 fiber optic gyrocompasses and 50 Y-690 units (electron tubes). Pursuant to that agreement, Ghahreman and his co-defendants wired approximately \$60,000 in partial payment for the gyrocompasses and electron tubes from a bank in Dubai to the undercover agents’ bank account. Ultimately, on Jun. 17, 2013, ICE-HSI agents arrested Ghahreman and Yildiz after they traveled to the U.S. and took partial delivery of one gyrocompass and two electron tubes and attempted to ship the items indirectly to Iran, via third countries. On Oct. 9, 2014, Yildiz pleaded guilty to conspiracy to export to Iran. He was sentenced on May 8, 2015, to time served, 2 years supervised release, and \$100 special assessment. On Jan. 21, 2016, the Court dismissed with prejudice the superseding indictment against Taherkhani and Tig Marine Engineering Services. This case was investigated by ICE-HSI and DCIS.

***Accelerometers to China*** – On Aug. 25, 2015, Yue Wu, a.k.a. David Wu, a Chinese national, was sentenced in the Western District of Washington to 18 months’ imprisonment, \$100 special assessment, and deportation after completion of his sentence following a plea of guilty on May 26, 2015, to conspiracy to violate the Arms Export Control Act. Previously, on Oct. 22, 2014, Wu was indicted for violating the Arms Export Control Act. According to court documents, between Dec. 2011, and Oct. 2014, Wu directed others to contact a United States manufacturer and request the purchase of QA3000 accelerometers for export to China without first obtaining a license from the United States Department of State. Wu and another person met with an undercover agent in San Francisco, CA, in an effort to order 30 accelerometers from the undercover agent. Wu explained that he was attempting to acquire the accelerometers on behalf of a customer in China. He requested that the accelerometers be concealed in housing to evade United States export restrictions, providing the agent with schematics for the construction of the housing. Court documents further show that Wu suggested that the agent ship the accelerometers to Wu’s associate in Switzerland, who, in turn, would transship the accelerometers into China.

***Firearms Parts and Accessories to Lebanon*** – On Aug. 12, 2015, in the District of Maryland, Sam Rafic Ghanem was sentenced to 18 months in prison followed by three years of supervised release for attempting to illegally export firearms parts and accessories to Lebanon, and for smuggling goods from the United States. Ghanem was ordered by the Court to pay a fine of \$70,734.24. Ghanem, a naturalized U.S. citizen born in Lebanon, owned and operated Washington Movers International, also known as Washington Movers, Inc., a freight forwarding business located in District Heights, Maryland. According to evidence presented at his five-day

trial, beginning Oct. 3, 2013, Ghanem sought to export guns and accessories to Lebanon through his shipping company that were provided to him by an FBI source. Ghanem knew that the weapons and accessories were designated as defense articles and required an export license, which Ghanem never sought or obtained. In addition, those items were prohibited from export to Lebanon. Specifically, Ghanem attempted to export seven 9mm semi-automatic pistols; three .40 caliber semi-automatic pistols; 10 AR-15 .223 caliber semi-automatic rifles; and 18 advanced combat optic gun sights. According to trial evidence, on Nov. 21, 2013, Ghanem told the source to pay him \$3,000 for the cost of purchasing salvaged vehicles which would be used to export the firearms and accessories. Ghanem texted the source his bank account number and at the direction of law enforcement, the source deposited \$3,000 into Ghanem's account. Ghanem purchased the salvaged vehicles and arranged for them to be cut up. Ghanem concealed the weapons and other items within the doors and cut-up parts of the salvaged vehicles, which were then loaded into a shipping container. Ghanem advised the source that the shipping container would be loaded with the remaining car parts and transported to the Port of Baltimore for shipment to Lebanon on Dec. 23, 2013. Ghanem was subsequently arrested. This investigation was conducted by the FBI and ICE HSI.

***Thermal Imaging Camera to Pakistan*** – On Jun. 30, 2015, in the Northern District of Illinois, Bilal Ahmed was sentenced to 24 months' imprisonment, \$100 special assessment, \$1,000 fine, and 2 years supervised release after previously pleading guilty on Oct. 2, 2014, to count one of a superseding indictment charging him with violating export control regulations. Previously, on May 7, 2014, a federal indictment was returned charging Ahmed with one count of violating the International Emergency Economic Powers Act (IEEPA) and one count of attempted smuggling of goods, in violation of U.S. export regulations. The indictment alleged that Ahmed violated U.S. export laws by attempting to ship a FLIR HRC-U thermal imaging camera from his company in Schaumburg, IL, to a company in Pakistan without first obtaining a license from the U.S. Commerce Department. The FLIR HRC-U thermal imaging camera is on the Commerce Control List and is controlled for reasons of national security and regional stability. Ahmed was initially charged in a criminal complaint and arrested on Mar. 14, 2014. According to the complaint affidavit and the indictment, Ahmed was the owner, president, and registered agent of Trexim Corp., which used the address of a virtual office in Schaumburg. Between Nov. 2013, and Feb. 2014, Ahmed corresponded via email with a company in California and negotiated the purchase of a FLIR HRC-U thermal imaging camera for approximately \$102,000, which he paid with two checks in Feb. 2014. Ahmed took delivery of the camera on Feb. 27, 2014, at a commercial shipping store in Bolingbrook, IL. On Mar. 7, 2014, Ahmed allegedly took the camera, packaged in two boxes, to a different commercial shipper located in Elk Grove Village and left the packages to be shipped to a company in Pakistan. The waybill included a handwritten note containing the letters "NLR," meaning "no license required." A search of U.S. State and Commerce Department databases showed there were no licenses applied for or obtained by Ahmed, Trexim or any other related individual or company names for the export of a FLIR HRC-U thermal imaging camera from the U.S. to Pakistan. This case was investigated by the Federal Bureau of Investigation and the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement.

***Theft of Trade Secrets by Chinese Professors for Technology to China*** - On May 16, 2015, Tianjin University Professor Hao Zhang was arrested upon entry into the U.S. from the People's Republic of China (PRC) in connection with a recent superseding indictment in the Northern District of California. The 32-count indictment, which had previously been sealed, charges a total of six individuals with economic espionage and theft of trade secrets for their roles in a long-running effort to obtain U.S. trade secrets for the benefit of universities and companies controlled by the PRC government. According to the indictment, PRC nationals Wei Pang and Zhang met at

a U.S. university in Southern California during their doctoral studies in electrical engineering. While there, Pang and Zhang conducted research and development on thin-film bulk acoustic resonator (FBAR) technology under funding from U.S. Defense Advanced Research Projects Agency (DARPA). After earning their doctorate in approximately 2005, Pang accepted employment as an FBAR engineer with Avago Technologies (Avago) in Colorado and Zhang accepted employment as an FBAR engineer with Skyworks Solutions Inc. (Skyworks) in Massachusetts. The stolen trade secrets alleged in the indictment belong to Avago or Skyworks. Avago is a designer, developer and global supplier of FBAR technology, which is a specific type of radio frequency (RF) filter. Throughout Zhang's employment, Skyworks was also a designer and developer of FBAR technology. FBAR technology is primarily used in mobile devices like cellular telephones, tablets and GPS devices. FBAR technology filters incoming and outgoing wireless signals so that a user only receives and transmits the specific communications intended by the user. Apart from consumer applications, FBAR technology has numerous applications for a variety of military and defense communications technologies. According to the indictment, in 2006 and 2007, Pang, Zhang and other co-conspirators prepared a business plan and began soliciting PRC universities and others, seeking opportunities to start manufacturing FBAR technology in China. Through efforts outlined in the superseding indictment, Pang, Zhang and others established relationships with officials from Tianjin University. Tianjin University is a leading PRC Ministry of Education University located in the PRC and one of the oldest universities in China. As set forth in the indictment, in 2008, officials from Tianjin University flew to San Jose, CA, to meet with Pang, Zhang and other co-conspirators. Shortly thereafter, Tianjin University agreed to support Pang, Zhang and others in establishing an FBAR fabrication facility in the PRC. Pang and Zhang continued to work for Avago and Skyworks in close coordination with Tianjin University. In mid-2009, both Pang and Zhang simultaneously resigned from the U.S. companies and accepted positions as full professors at Tianjin University. Tianjin University later formed a joint venture with Pang, Zhang and others under the company name ROFS Microsystem intending to mass produce FBARs. The indictment alleged that Pang, Zhang and other co-conspirators stole recipes, source code, specifications, presentations, design layouts and other documents marked as confidential and proprietary from the victim companies and shared the information with one another and with individuals working for Tianjin University. According to the indictment, the stolen trade secrets enabled Tianjin University to construct and equip a state-of-the-art FBAR fabrication facility, to open ROFS Microsystems, a joint venture located in PRC state-sponsored Tianjin Economic Development Area (TEDA), and to obtain contracts for providing FBARs to commercial and military entities. The remaining indicted defendants are all citizens of the PRC and include: Jinping Chen, a professor at Tianjin University and a member of the board of directors for ROFS Microsystems; Huisui Zhang (Huisui) studied with Pang and Zhang at a U.S. university in Southern California and received a Master's Degree in Electrical Engineering in 2006; Chong Zhou, a Tianjin University graduate student and a design engineer at ROFS Microsystem. Zhou studied under Pang and Zhang; Zhao Gang, the General Manager of ROFS Microsystems. This investigation was conducted by the FBI.

***Illegal Trade with Iran and Sudan*** – On May 6, 2015, in the District of Columbia, Schlumberger Oilfield Holdings Ltd. (SOHL), a wholly-owned subsidiary of Schlumberger Ltd., entered into a formal judgment memorializing the sentence requiring SOHL to pay a \$232,708,356 penalty to the U.S. for conspiring to violate the International Emergency Economic Powers Act (IEEPA) by willfully facilitating illegal transactions and engaging in trade with Iran and Sudan. At a hearing on Apr. 30, 2015, the Court accepted the company's guilty plea and sentenced the company to the proposed sentence articulated in the plea agreement, which called for the fine and other terms of corporate probation. The court recognized the seriousness of SOHL's criminal conduct, which posed a threat to our national security. In addition, the court noted that the scope of criminal

conduct justified the large monetary penalty imposed. Finally, the court concluded that the terms of probation provided adequate deterrence to SOHL as well as other companies. The Court entered the written judgment confirming the sentence imposed on Apr. 30, 2015. Previously, on Mar. 25, 2015, a criminal information was filed in the District of Columbia charging SOHL with one count of knowingly and willfully conspiring to violate IEEPA. SOHL waived the requirement of being charged by way of federal Indictment, agreed to the filing of the information, and accepted responsibility for its criminal conduct and that of its employees by entering into a plea agreement with the government. The plea agreement requires that SOHL pay the U.S. government \$232,708,356 and enter into a three-year period of corporate probation. SOHL's monetary penalty includes a \$77,569,452 criminal forfeiture and an additional \$155,138,904 criminal fine. The criminal fine represents the largest criminal fine in connection with an IEEPA prosecution. In addition to SOHL's agreement to continue its cooperation with U.S. authorities throughout the three-year period of probation and not to engage in any felony violation of U.S. federal law, SOHL's parent company, Schlumberger Ltd., also has agreed to continue its cooperation with U.S. authorities during the three-year period of probation, and hire an independent consultant who will review the parent company's internal sanctions policies, procedures and company-generated sanctions audit reports. According to court documents, starting in or about early 2004 and continuing through Jun. 2010, Drilling & Measurements (D&M), a United States-based Schlumberger business segment, provided oilfield services to Schlumberger customers in Iran and Sudan through non-U.S. subsidiaries of SOHL. Although SOHL, as a subsidiary of Schlumberger Ltd., had policies and procedures designed to ensure that D&M did not violate U.S. sanctions, SOHL failed to train its employees adequately to ensure that all U.S. persons, including non-U.S. citizens who resided in the United States while employed at D&M, complied with Schlumberger Ltd.'s sanctions policies and compliance procedures. As a result of D&M's lack of adherence to U.S. sanctions combined with SOHL's failure to train properly U.S. persons and to enforce fully its policies and procedures, D&M, through the acts of employees residing in the United States, violated U.S. sanctions against Iran and Sudan by: (1) approving and disguising the company's capital expenditure requests from Iran and Sudan for the manufacture of new oilfield drilling tools and for the spending of money for certain company purchases; (2) making and implementing business decisions specifically concerning Iran and Sudan; and (3) providing certain technical services and expertise in order to troubleshoot mechanical failures and to sustain expensive drilling tools and related equipment in Iran and Sudan. In 2009, in consultation with the U.S. Department of State, Schlumberger agreed to no longer pursue new oilfield contracts in Iran. In 2011, Schlumberger voluntarily decided to cease providing oilfield services in Iran and the Republic of the Sudan (North Sudan). As of Jun. 30, 2013, Schlumberger ceased providing oilfield services in Iran. And presently, Schlumberger has ceased providing oilfield services in North Sudan as well. This case was investigated by the Department of Commerce – BIS.

***Trade Secrets to South Korea*** - On May 1, 2015, Kolon Industries, Inc., a South Korean industrial company, was sentenced in the Eastern District of Virginia to 5 years' probation and was ordered to pay \$400 special assessment, \$85,000,000 in criminal fines and \$275,000,000 in restitution. Kolon Industries, Inc., appearing through two successor entities—Kolon Industries, Inc. and Kolon Corporation (collectively, Kolon)—pleaded guilty in federal court on Apr. 30, 2015, to one count of conspiracy to convert trade secrets involving E.I. DuPont de Nemours & Co.'s (DuPont) Kevlar technology. According to the statement of facts filed with the plea agreement, from Jun. 2006, to Feb. 2009, Kolon conspired with former DuPont employees and others to steal DuPont's trade secrets for making Kevlar, a high-strength, para-aramid synthetic fiber. Kevlar, a trademarked name, is one of DuPont's most well-known products and is used in a wide range of commercial applications such as body armor, fiber optic cables, and automotive and industrial products. Kolon admitted that it was attempting to improve the quality of its own

para-aramid fiber known as Heracron. Kolon personnel met repeatedly with former DuPont employees, including Edward Schulz of Brownstown, PA, and Michael Mitchell, of Chesterfield, VA, to obtain confidential and proprietary DuPont information about Kevlar. Schulz pleaded guilty to conspiracy to steal trade secrets in Sep. 2014, and was sentenced in Jul. 2015, to 2 years' probation, 500 hours' community service, \$100 special assessment and a \$75,000 fine. Mitchell pleaded guilty to theft of trade secrets and obstruction of justice in Dec. 2009, and was sentenced to 18 months in prison, 3 years supervised release, \$200 special assessment, and \$187,895.90 in restitution. Kolon admitted that it obtained technical and business documents regarding Kevlar, including instructional materials that described DuPont's "New Fiber Technology," documents on polymerization, and a detailed breakdown of DuPont's capabilities and costs for the full line of its Kevlar products and DuPont's Kevlar customers. According to the statement of facts and Mitchell's admissions at his guilty plea, Mitchell exchanged numerous telephone calls and emails with Kolon personnel. On more than one occasion, Mitchell advised Kolon personnel that some of the information they sought was proprietary and that DuPont considered such information to be trade secrets. Mitchell also coordinated a meeting at a hotel in Richmond, at which Kolon personnel were introduced to a cooperating witness who pretended to be a disgruntled scientist from DuPont. During the Richmond meeting, Kolon personnel indicated that they would only be comfortable communicating with the cooperating witness in a manner that was confidential and that would not leave an evidentiary trail. In Feb. 2009, DuPont filed a civil lawsuit against Kolon in the Eastern District of Virginia, alleging theft of trade secrets. Thereafter, certain Kolon personnel attempted to delete files and emails related to Mitchell, Schulz and outside consultants hired to improve Kolon's para-aramid fiber, and urged other Kolon personnel to search for such materials and mark them for deletion. Kolon also admitted that certain employees approached a former employee of an American subsidiary of Teijin Ltd. – a Japanese company that makes the para-aramid fiber called Twaron—in an unsuccessful effort to obtain information about Twaron. This case represents the first time that foreign corporations with no direct presence in the United States were found to be successfully served with U.S. criminal process, over their objections, based on service pursuant to an international treaty. In Dec. 2014, the district court found that both of the successor companies were properly served, and ordered them to appear for arraignment. In Feb. 2015, the Fourth Circuit Court of Appeals denied Kolon's petition for extraordinary relief seeking reversal of the district court's order. Five former Kolon executives and employees, all of South Korea, were charged in an Aug. 2012, indictment filed in the Eastern District of Virginia: Jong-Hyun Choi, a senior executive who oversaw the Heracron Business Team; In-Sik Han, who managed Kolon's research and development related to Heracron; Kyeong-Hwan Rho, the head of the Heracron Technical Team; Young-Soo Seo, the general manager for the Heracron Business Team; and Ju-Wan Kim, a manager on the Heracron Business Team. The case was investigated by the FBI's Richmond Division.

***Fighter Jet Parts to Thailand and Pakistan*** - On Apr. 27, 2015, Russell Marshall and his company, Universal Industries Limited, Inc., were sentenced in the Southern District of Florida for violating the International Emergency Economic Powers Act. Marshall was sentenced to serve 41 months in prison and will be removed from the United States upon the completion of his sentence. In imposing the sentence, the Court found that the order denying export privileges issued by the Department of Commerce constituted a national security control, which subjected Marshall to an enhanced sentence. Marshall and his company, Universal Industries Limited Inc., were previously convicted in a 2011 case in the Southern District of Florida for violating the Arms Export Control Act, after which the Department of Commerce issued a denial order prohibiting Universal Industries Limited Inc. and its owners, agents and employees from participating in any transaction involving the export of any item subject to the Department of Commerce's Export Administration Regulations (EAR). Marshall and Universal Industries Limited Inc. violated IEEPA and the U.S. Department of Commerce's denial order by attempting

to send three temperature transmitters used on F-16 fighter jets and a saddle part for the J-69 engine used on 737 military trainer aircraft to Thailand and Pakistan, respectively. According to court documents and information presented during the sentencing hearing, the DoD Inspector General received a hotline complaint concerning Marshall and Universal Industries Limited Inc. in Nov. 2012. The subsequent investigation revealed that the defendants brokered the sale of military aircraft parts which were subject to license controls by the Department of Commerce, and which the defendants knew were intended to be illegally exported to Thailand and Pakistan. On Feb. 6, 2015, Marshall and Universal Industries Limited Inc. entered guilty pleas to an information that charged them with knowingly and willfully engaging in negotiations concerning selling, delivering or otherwise servicing a transaction involving an item to be exported from the United States to Thailand and subject to the EAR. Universal Industries Limited Inc. was sentenced to a term of one year of probation and a special assessment of \$400 upon a finding that the corporation is currently listed as inactive by the Florida Division of Corporations as a result of Marshall's arrest. This case was investigated by DoD, DCIS, ICE-HSI and the U.S. Department of Commerce's Office of Export Enforcement.

**WMD Materials to North Korea** –On Apr. 24, 2015, Yueh-Hsun Tsai, a.k.a. “Gary Tsai”, was sentenced in the Northern District of Illinois to 3 years of probation and a fine of \$250. On Mar. 16, 2015, Hsien Tai Tsai, a.k.a. “Alex Tsai”, was sentenced to 2 years’ imprisonment and \$100 special assessment. Previously, on Oct. 10, 2014, Alex Tsai pleaded guilty to conspiracy to defraud the United States in its enforcement of regulations targeting proliferators of weapons of mass destruction. In his plea agreement, Alex Tsai admitted that he engaged in illegal business transactions involving the export of U.S. origin goods and machinery. On Dec. 16, 2014, his son, Gary Tsai, pleaded guilty to a superseding information charging him with making a false bill of lading. In his plea agreement, Gary Tsai admitted to arranging the export of a grinder to Taiwan by falsely identifying the consignee of the shipment. On Jun. 6, 2013, Alex Tsai, who the U.S. government has linked to the supply of weapons machinery to North Korea, and Gary Tsai, were indicted in the Northern District of Illinois for allegedly conspiring to violate U.S. laws designed to thwart the proliferation of weapons of mass destruction. On May 1, 2013, both Alex Tsai and Gary Tsai were arrested pursuant to criminal complaints filed on Apr. 19, 2013. Alex Tsai, who was believed to have resided in Taiwan, was arrested in Tallinn, Estonia, and later extradited to the United States. Gary Tsai, who is from Taiwan and is a U.S. legal permanent resident, was arrested at his home in Illinois. Each were charged with conspiring to defraud the United States in its enforcement of laws prohibiting the proliferation of weapons of mass destruction; conspiracy to violate the International Emergency Economic Powers Act (IEEPA) by conspiring to evade the restrictions imposed on Alex Tsai and two of his companies by the U.S. Treasury Department, and money laundering. Agents had been investigating the pair, as well as Individual A (a Taiwanese associate of Alex Tsai), and a network of companies engaged in the export of U.S. origin goods and machinery that could be used to produce weapons of mass destruction. The investigation revealed that Alex and Gary Tsai and Individual A were associated with at least three companies based in Taiwan - Global Interface Company, Inc., Trans Merits Co., Ltd., and Trans Multi Mechanics Co., Ltd. - that purchased and then exported, and attempted to purchase and then export, from the United States machinery used to fabricate metals and other materials with a high degree of precision. On Jan. 16, 2009, the Treasury Department designated Alex Tsai, Global Interface, and Trans Merits as proliferators of weapons of mass destruction, isolating them from the U.S. financial system and prohibiting any U.S. person or company from doing business with them. In announcing the order, the Treasury Department said that Alex Tsai was designated for providing support for, or goods or services in support of the Korea Mining Development Trading Corporation (KOMID), which was designated as a proliferator by the U.S. in 2005. The Treasury Department asserted that Alex Tsai "has been supplying goods with weapons production capabilities to KOMID and its subordinates since the late 1990s, and he has



been involved in shipping items to North Korea that could be used to support North Korea's advanced weapons program." After the OFAC designations, Alex and Gary Tsai and another individual allegedly continued to conduct business together but attempted to hide Alex Tsai's and Trans Merit's involvement in those transactions by conducting business under different company names, including Trans Multi Mechanics. This investigation was conducted by the FBI, ICE-HSI and BIS.

***Military Sensors Manufactured for Department of Defense Exported to China*** – On Apr. 23, 2015, Bo Cai, a Chinese national, was sentenced in the District of New Mexico to 24 months' imprisonment. On the same day, his cousin Wentong Cai, a Chinese national in the U.S. on a student Visa, was also sentenced to 18 months' imprisonment. Both men are scheduled to be deported after completing their prison sentences. Bo Cai and Wentong Cai were charged in a three-count superseding indictment with a scheme to illegally export sensors primarily manufactured for sale to the U.S. Department of Defense for use in high-level applications such as line-of-sight stabilization and precision motion control systems, without first obtaining the required export license. Previously, on Dec. 16, 2014, Wentong Cai, pleaded guilty to conspiring with Bo Cai to violate the Arms Export Control Act and the International Traffic Arms Regulations (ITAR). Bo Cai pleaded guilty on Jul. 23, 2014. Cai and Wentong Cai participated in a scheme to illegally export defense articles with military applications to the People's Republic of China. According to court documents, in Mar. 2012, Bo Cai, was employed by a technology company in China. He embarked on an illegal scheme to smuggle sensors out of the U.S. to China for one of his customers despite knowledge that the sensors could not be exported without a license and that the U.S. did not issue licenses to export the sensors to China. Bo Cai enlisted his cousin Wentong Cai to acquire the sensors under the ruse that he planned to use the sensors at Iowa State University where he was a graduate microbiology student. The investigation of this case began in Oct. 2013, when an undercover HSI agent responded to Wentong Cai's overtures. After negotiations by telephone and email, Bo Cai and Wentong Cai traveled to New Mexico in Dec. 2013, where they obtained a sensor from undercover HSI agents and developed a plan for smuggling the sensor out of the U.S. to China. On Dec. 11, 2013, Bo Cai was arrested at an airport in Los Angeles, CA, after the sensor was discovered concealed in a computer speaker in his luggage. Bo Cai was preparing to board a flight to China. Wentong Cai was arrested in Iowa in Jan. 2014. This investigation was conducted by Homeland Security Investigations, USAF Office of Special Investigations, Defense Security Service, FBI.

***High-Tech Microelectronics and Uninterruptible Power Supplies to Iran*** – On Apr. 17, 2015, in the Southern District of Texas, a 24-count indictment was unsealed charging four corporations and five individuals with facilitating the illegal export of high-tech microelectronics, uninterruptible power supplies and other commodities to Iran, in violation of the International Emergency Economic Powers Act (IEEPA). The indictment alleged that Houston-based company Smart Power Systems Inc. (SPS), Bahram Mechanic and Tooraj Faridi – both of Houston, and Khosrow Afghahi of Los Angeles, were all members of an Iranian procurement network operating in the United States. Also charged as part of the scheme were Arthur Shyu and the Hosoda Taiwan Limited Corporation in Taiwan, Matin Sadeghi and Golsad Istanbul Trading Ltd. in Turkey, and the Faratel Corporation co-owned by Mechanic and Afghahi in Iran. The indictment was returned under seal on Apr. 16, 2015, and unsealed as Mechanic and Faridi made their initial appearances. Afghahi was taken into custody and made an initial appearance in the Central District of California. Sadeghi and Shyu are believed to be out of the country. Warrants remain outstanding for their arrests. In conjunction with the unsealing of these charges, the Department of Commerce designated seven foreign nationals and companies, adding them to its Entity List. Designation on the Entity List imposes a license requirement before any commodities can be exported from the United States to these persons or companies and establishes a

presumption that no such license will be granted. According to the indictment, Mechanic and Afghahi are the co-owners of Iran-based Faratel and its Houston-based sister company SPS. Faratel, currently the vice president of SPS, designs and builds uninterruptible power supplies for various Iranian entities, including Iranian government agencies such as the Iranian Ministry of Defense, the Atomic Energy Organization of Iran, and the Iranian Centrifuge Technology Company. Shyu is a senior manager at the Hosoda Taiwan Limited Corporation, a trading company located in Taiwan, while Sadeghi is an employee of Golsad Istanbul Trading, a shipping company located in Turkey. The indictment alleged that between approximately Jul. 2010, and the present, Mechanic and the others engaged in a conspiracy to obtain various commodities, including controlled United States-origin microelectronics. They then allegedly exported these commodities to Iran, while carefully evading the government licensing system set up to control such exports. The microelectronics shipped to Iran allegedly included microcontrollers and digital signal processors. These commodities have various applications and are frequently used in a wide range of military systems, including surface-air and cruise missiles. Mechanic's network allegedly sent at least \$24 million worth of commodities to Iran. Mechanic, assisted by Afghahi and Faridi, regularly received lists of commodities, including United States-origin microelectronics sought by Faratel in Iran, and would approve these orders and then send the orders to Shyu in Taiwan. Shyu would allegedly purchase the commodities utilizing Hosoda Taiwan Limited and then ship the commodities to Turkey, where Sadeghi would act as a false buyer via his company, Golsad Istanbul Trading Ltd. The indictment further alleged that Sadeghi would receive the commodities from Shyu and then ship them to Faratel in Iran. Mechanic required his co-conspirators to notify him and obtain his approval for each of the transactions completed by the network. The individual defendants each face up to 20 years in federal prison, while the corporate defendants face fines of up to \$1 million for each of the IEEPA counts. Mechanic, Afghahi and Shyu are also charged with conspiring to commit money laundering and substantive money laundering violations, each charge carries a maximum federal prison term of 20 years. Mechanic further faces a charge of willful failure to file foreign bank and financial accounts for which he faces up to five years in federal prison. The charges also carry the possibility of substantial fines upon conviction. Arthur Shyu remains a fugitive. This case was investigated by the FBI, Department of Commerce, and the IRS.

***Computers to Iran*** – On Apr. 6, 2015, in the Northern District of Texas, Borna Faizy, of Frisco, Texas, and Touraj Ghavidel, of Plano, Texas -- the corporate owners/operators of Signal Microsystems in Addison, Texas, a company that sold computers domestically and internationally -- were both sentenced to 2 years' probation, \$100 special assessment and \$75,000 fine. Faizy and Ghavidel both pleaded guilty on Sept. 29, 2014, to making false statements to federal agents about the illegal export of computer equipment from the United States to Iran. Previously, on Mar. 7, 2013, Faizy and Ghavidel were arrested on an indictment alleging that they illegally shipped \$12 million worth of computer equipment to Iran through Dubai. The indictment, returned under seal in early Mar. 2013, charges each with one count of conspiracy to illegally export to Iran, nine substantive counts charging illegal export and attempted export of goods to Iran and one count of making false statements to a federal agency. Faizy and Ghavidel allegedly acquired computers from U.S. companies to supply to end-users in Iran and concealed from the U.S. that the computers were destined for Iran. Faizy and Ghavidel allegedly actively recruited Iranian customers by marketing their computer business to business owners and individuals in Iran, and, in 2008 or 2009, attended a computer trade show, known as "GITEX," in Dubai to recruit Iranian customers. The defendants allegedly used freight-forwarding companies in Dubai to ship the equipment to Iran and communicated with coconspirators using fictitious names and coded language to obscure the true identities and locations of the ultimate consignees and end-users. They also created invoices and export forms that falsely identified the ultimate consignees of the shipments as parties in Dubai. The investigation was conducted by members of the North

Texas Counter-proliferation Task Force, which includes the FBI, ICE, the Department of Commerce and DCIS.

***High-Powered Military-Grade Weapons to the Philippines*** – On Mar. 27, 2015, in the Eastern District of New York, two law enforcement officers who used their positions to obtain high-powered military-grade weapons to smuggle to the Philippines, were sentenced to three years in prison, followed by three years of supervised release. According to court documents, former New York City Police Officer Rex Maralit and his brother Wilfredo Maralit, a U.S. Customs and Border Protection officer assigned to Los Angeles International Airport, pleaded guilty on Jun. 12, 2014, for their roles in an illegal scheme to smuggle high-powered assault rifles, sniper rifles, pistols, and firearms accessories from the United States to the Philippines, violating the Arms Export Control Act. A third brother, Ariel Maralit, resides in the Philippines and remains a fugitive. Court documents further alleged that between Jan. 2009, and Sep. 2013, the defendants exported a variety of military-style firearms, along with high-capacity magazines and accessories for those weapons, from the United States to the Philippines, where they were sold to overseas customers. Both Rex and Wilfredo Maralit used their official credentials and status to obtain and ship the weapons without first obtaining a license from the U.S. State Department. The firearms included the Barrett .50 caliber long-range semi-automatic rifle, the FN “SCAR” assault rifle, and high-capacity FN 5.7mm semi-automatic carbines and pistols which fire a cartridge that was specifically designed to penetrate body armor. The Arms Export Control Act requires exporters of firearms to first obtain the approval of the U.S. State Department before shipping weapons overseas. Similarly, dealing in firearms is regulated by the ATF, which requires gun dealers to first obtain a federal firearms license before engaging in such a business. This case was investigated by U.S. Immigration and Customs Enforcement’s (ICE) Homeland Security Investigations (HSI), Defense Criminal Investigative Service (DCIS), Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and New York City Police Department (NYPD).

***Aluminum Tubes to Iran*** – On Mar. 4, 2015, Nicholas Kaiga of Brussels and London, was sentenced in the Northern District of Illinois to 27 months’ imprisonment, two years supervised release, and \$100 special assessment after a plea of guilty on Dec. 4, 2014, to one count of attempting to violate the export control regulations. Previously, on Oct. 24, 2013, a federal grand jury returned a three -count indictment charging Kaiga with one count of violating the International Emergency Economic Powers Act (IEEPA) and two counts of making false statements on U.S. export forms. The defendant allegedly attempted to export aluminum tubes that were controlled for nuclear nonproliferation purposes from a company in Schaumburg, through Belgium, to a company in Kuala Lumpur, Malaysia, without obtaining a license from the U.S. Commerce Department. According to the complaint affidavit and indictment, the Schaumburg company, identified as "Company A" in court documents, began cooperating with law enforcement in Dec. 2007. The cooperation began after a person identified as "Individual A," who was at times located in Iran, attempted to purchase 7075 aluminum from Company A, to be shipped to a company in the United Arab Emirates, but was denied an export license. In late 2009, an undercover agent began posing as an employee of Company A. Between Nov. 2009, and Feb. 2012, the indictment alleged that Kaiga, who was managing director of a Belgian company, Industrial Metals and Commodities, attempted to export 7075 aluminum from Company A to Company B in Malaysia without an export license. The complaint affidavit alleged that Company B was a front for Individual A in Iran. The false statements charges allege that Kaiga lied on Commerce Department export declaration forms, which stated that the ultimate destination and recipient of the 7075 aluminum were in Belgium. In Nov. 2011, material that was purported to be 7075 aluminum, but was actually substituted with a different aluminum by Company A in cooperation with law enforcement, was picked up from Company A by a freight forwarding company designated by Kaiga's Belgian company. The material arrived in the

Belgian port of Antwerp on Dec. 1, 2011, and two months later it was shipped by a freight forwarding company to Individual A's front company in Malaysia. This investigation was conducted by HSI, FBI, BIS, and OEE.

***Oilfield Service Equipment to Iran*** – On Feb. 24, 2015, Patrick Jean Zuber, a lawful permanent resident of the U.S., was sentenced in the Southern District of Texas to one year of probation, \$100 special assessment and a \$15,000 fine. Previously, on Sep. 24, 2014, Zuber pleaded guilty to a Criminal Information charging him with conspiracy to smuggle oilfield service equipment from the United States to Iran. Zuber was the Vice President of Middle East and North Africa (MENA) East where he oversaw the operations in India, Saudi Arabia, Yemen, Oman, Qatar, Turkmenistan, and Pakistan for Weatherford Oil Tool Middle East Limited (WOTME), a wholly owned subsidiary of Weatherford International, Ltd. (Weatherford), one of the world's largest oilfield service companies. According to court documents, in Jan. 2007, Zuber received an email from a Weatherford manager operating in Thailand asking about services Weatherford could provide in Iran. Zuber forwarded the request to a Canadian citizen who was Vice President of MENA West and responsible for Weatherford's sales to Iran. Zuber did this while knowing that facilitating the sale of equipment through the United Arab Emirates and on to Iran was illegal under United States law.

***Military Articles to China*** – On Feb. 18, 2015, in the Northern District of Illinois, an indictment was made public charging an Arlington Heights company, its president, and a former employee with unlawfully exporting and importing military articles, including components used in night vision systems and on the M1A1 Abrams tank, which is the main battle tank used by the U.S. Armed Forces. The defendants were charged in an indictment returned by a federal grand jury on Jan. 14, 2015. Defendant Vibgyor Optical Systems, Inc. purported to manufacture optics and optical systems, including items that were to be supplied to the U.S. Department of Defense (DOD). Instead of manufacturing the items domestically, as it claimed, Vibgyor illegally sent the technical data for, and samples of, the military articles to manufacturers in China, then imported the items from China to sell to its customers – including DOD prime contractors. Vibgyor's president, Bharat "Victor" Verma, and Urvashi "Sonia" Verma, a former Vibgyor employee and owner of a now-defunct company that operated as a subcontractor for Vibgyor, were also charged in the indictment. According to the indictment, between Nov. 2006, and Mar. 2014, the defendants conspired to defraud the United States and violate both the Arms Export Control Act (AECA) and International Traffic in Arms Regulations (ITAR). Vibgyor won subcontracts to supply optical components and systems to DOD prime contractors by misrepresenting the location of the manufacture of the items it supplied. Bharat Verma falsely claimed that the items Vibgyor supplied were manufactured domestically, when they actually had been manufactured in China, based on information illegally exported to Chinese manufacturers. In addition to illegally providing technical data for a military item to China, Urvashi Verma attempted to ship an example of one of the military items to the Chinese manufacturer. Vibgyor, Bharat Verma, and Urvashi Verma are charged with one count of conspiracy to violate both the AECA and the ITAR, one count of conspiracy to defraud the United States, and one count of violating the AECA. Vibgyor and Bharat Verma were also charged with international money laundering. Trial is scheduled to begin in Apr. 2017. This case was investigated by Homeland Security Investigations, Internal Revenue Service, Department of Defense Criminal Investigative Service.

***Military Night Vision Devices Overseas*** – On Feb. 9, 2015, in the District of Maryland, David Kelley was sentenced to 18 months in prison followed by three years of supervised release after a plea of guilty on May 9, 2014, for the unlawful export of arms and munitions, specifically, night vision devices, in violation of 22 U.S.C. § 2778. According to his plea agreement, Kelley ran a business named "Optical Solutions and More" that sold night vision and other military-style

items, primarily over eBay. Kelley entered into distributor agreements with night vision manufacturers in which he acknowledged that he was aware of restrictions known as the International Traffic in Arms Regulations (ITAR), 22 C.F.R. §§ 120-130, which prohibited the unlicensed export of U.S. munitions list items, including the export of night vision devices using Generations 2 and newer technology. After entering into these agreements, Kelley discussed circumventing ITAR restrictions with foreign customers who responded to his internet listings. Between May 2011, and Feb. 2012, Kelley made approximately 60 shipments containing ITAR-restricted weapons parts and night vision devices destined for customers in 24 countries, including Argentina, Australia, Russia, the Philippines, United Kingdom and Japan. To disguise the ITAR violations, Kelley variously labeled these shipments as "toys," "toy blocks," "spotting scope," and "monocular parts." In exchange for these shipments, Kelley collected over \$140,000 in 150 separate PayPal transactions. In Sep. 2011, an undercover HSI agent located in Baltimore posed as a buyer from New Zealand and contacted Kelley to ask if Kelley would export an ATN Generation 4 Monocular Night Vision Device. Kelley acknowledged in an email that such an export violated ITAR and demanded additional payment for risking prosecution. On Oct. 24, 2011, Kelley exported the device, which is designated as a defense article on the U.S. munitions list, to New Zealand, without first obtaining a license from the State Department.

***Industrial Products to Iran*** – On Feb. 2, 2015, in the District of Maryland, Ali Saboonchi, a U.S. citizen, was sentenced to 2 years in prison, 1 year supervised release, and \$800 special assessment. Previously, on Aug. 11, 2014, a federal jury convicted Saboonchi of conspiracy and seven counts of exporting U.S. manufactured industrial products and services to Iran, in violation of the International Emergency Economic Powers Act. On Mar. 7, 2013, an indictment was unsealed charging Saboonchi and Arash Rashti Mohammad, a citizen and resident of Iran, with conspiracy to export and exporting U.S. manufactured industrial products and services to Iran. The indictment was returned on Mar. 4, 2013, and unsealed upon Saboonchi's arrest. From Nov. 2009, to the present, Saboonchi and Rashti conspired to evade the Iranian embargo by exporting U.S. manufactured industrial goods and services to Iranian businesses. Rashti, located in Iran, allegedly asked Saboonchi, located in Maryland, to create and operate Ace Electric Company for the purpose of obtaining goods to send to Iran. Rashti, who operated businesses in Iran and the United Arab Emirates (UAE), allegedly solicited business from customers in Iran for industrial parts and components manufactured in the United States. Saboonchi obtained price quotes, paid for, and took delivery of most of the U.S. goods. He then caused the goods to be shipped to co-conspirators in UAE, and in at least one case, China. Rashti would repay Saboonchi and then arrange for the entities in the UAE and China to send the goods to him and his customers in Iran. Finally, the defendants did not obtain a license or authorization to export these goods to Iran. Rashti remains at large. On Aug. 9, 2016, the Court dismissed the indictment against Rashti, Mehdi Mohammadi, and Eshan Naghshineh. The investigation was conducted by the FBI and ICE.

***Sanctions Violations to Aid Zimbabwean Government Officials*** – On Jan. 21, 2015, C. Gregory Turner, also known as Greg Turner, was sentenced in the Northern District of Illinois to 15 months in prison, one year supervised release, \$100 special assessment, and a fine of \$90,000. Previously, on Oct. 10, 2014, Turner was convicted by a federal jury of conspiracy to violate the International Emergency Economic Powers Act (IEEPA) from late 2008 through early 2010 by agreeing to assist Zimbabwe President Robert Mugabe and others in an effort to lift economic sanctions against Zimbabwe. Turner met multiple times in the United States and in Africa with Zimbabwean government officials, including President Mugabe and Gideon Gono, governor of the Reserve Bank of Zimbabwe, who were individually subject to U.S. sanctions. A Nov. 2008, consulting agreement provided for a total payment of \$3.4 million in fees for Turner and his co-defendant, Prince Asiel Ben Israel, to engage in public relations, political consulting, and

lobbying efforts to have sanctions removed by meeting with and attempting to persuade federal and state government officials, including Illinois members of Congress and state legislators, to oppose the sanctions. President Mugabe and his ruling ZANU-PF party have governed Zimbabwe since its independence in 1980. The sanctions against President Mugabe and other specially designated individuals in Zimbabwe – for human rights abuses – neither bar travel to Zimbabwe nor prohibit public officials from meeting with specially designated nationals to discuss removing the sanctions. But, individuals may not provide services on behalf of or for the benefit of specially designated nationals. According to the evidence at trial, in early Nov. 2008, Turner and Ben Israel began having discussions with Mugabe, Gono, and other ZANU-PF leaders regarding the influence Turner and Ben Israel could wield to have the sanctions removed. The defendants discussed with President Mugabe, Gono, and others their association with many public officials who purportedly had close connections with then President-Elect Obama. Turner violated IEEPA by conspiring to engage in public relations, political consulting, and lobbying efforts on behalf of President Mugabe and other Zimbabwe officials. In early Dec. 2008, Ben Israel's U.S. bank blocked a wire transfer of \$89,970 into his account from a Zimbabwean official affiliated with ZANU-PF; and, Ben Israel later traveled to Africa and personally withdrew \$90,000 from the bank account of that same Zimbabwean official. Turner and Ben Israel arranged for trips by federal and state government officials to meet with President Mugabe and other Zimbabwean officials, including in Nov. and Dec. 2008, and Jan. and Dec. 2009; attempted to have Gono and other Zimbabwean officials speak at an issues forum in Washington, D.C., sponsored by a then-U.S. Representative from California, and to assist those officials in obtaining visas to travel to the U.S. to attend the event; arranged for President Mugabe to meet with federal and state government officials in New York; lobbied a caucus of state legislators on behalf of Zimbabwean officials; and failed to apply to the Treasury Department for a license to engage in transactions and services on behalf of specially designated nationals. In early Dec. 2008, Turner and Ben Israel arranged for a delegation to travel to Zimbabwe. After members of the delegation returned, President-Elect Obama's transition team forwarded information about contact from a member of the delegation to the FBI based on its concerns that sanctions may have been violated by traveling to Zimbabwe, which was not itself prohibited. Throughout 2009, Turner and Ben Israel continued to pass communications between Zimbabwean leaders and, purportedly, U.S. public officials while seeking payment for their services from Gono. Ben Israel was sentenced on Aug. 21, 2014, to seven months in prison, one year supervised release, \$100 special assessment and a \$500 fine after pleading guilty to violating the Foreign Agents Registration Act (FARA). This case was investigated by the Federal Bureau of Investigation and the Internal Revenue Service Criminal Investigation Division.

***Lockheed Martin Fuel Quantity Indicators to Malaysia*** – On Jan. 13, 2015, in the District of New Hampshire, Netria Corporation was sentenced to one year of probation and ordered to forfeit \$12,560. On Oct. 2, 2014, Netria pleaded guilty to a one-count Information charging it with exporting without a license two Lockheed Martin Fuel Quantity Indicators, which are defense articles on the Munitions List, in violation of the Arms Export Control Act (AECA). According to court documents, in Sep. 2008, a domestic undercover storefront received a request from a Netria employee for a quote for a Northrup Grumman F-14 Tomcat fighter aircraft part. Subsequent to the request, federal agents began an investigation into Netria's sales and export activities. During the course of the investigation, it was discovered that Netria had made sales and exports of numerous shipments of parts belonging to the Lockheed Martin C-130 Hercules military aircraft. A portion of those sales and exports consisted of parts and equipment which were classified as defense articles under the AECA and require a license from the Department of State prior to export out of the United States. In all, Netria exported nine shipments of C-130 parts from Sep. 2008, through Apr. 2009, without a license and brokered the sale and export of

approximately \$2 million in such aerospace parts between Jul. 2007, and Oct. 2009. This case was investigated by ICE/HSI and DCIS.

***Drone, Missile and Stealth Technology to China*** – On Jan. 9, 2015, Hui Sheng Shen, a.k.a. Charlie, was sentenced in the District of New Jersey to 49 months in prison and \$200 special assessment. On Jan. 6, 2015, Huan Ling Chang, a.k.a. “Alice” was sentenced to time served and \$200 special assessment. Previously, on Sep. 22, 2014, Shen and Chang, both Taiwanese nationals, each pleaded guilty to one count of conspiracy to violate the Arms Export Control Act and one count of conspiracy to import illegal drugs. On Apr. 25, 2012, Shen and Chang were charged separately by amended criminal complaints with conspiracy to violate the Arms Export Control Act. The defendants were arrested on Feb. 25, 2012, in New York in connection with a complaint in New Jersey charging them with conspiring to import and importing crystal methamphetamine from Taiwan to the United States. According to the amended complaint, during negotiations with undercover FBI agents over the meth deal, the defendants asked FBI undercover agents if they could obtain an E-2 Hawkeye reconnaissance aircraft for a customer in China. In subsequent conversations, Shen and Chang allegedly indicated they were also interested in stealth technology for the F-22 fighter jet, as well missile engine technology, and various Unmanned Aerial Vehicles (UAV), including the RQ-11b Raven, a small, hand-launched UAV used by the U.S. Armed Forces. Shen and Chang allegedly stated that their clients were connected to the Chinese government and its intelligence service. According to the complaint, they sent undercover agents a code book to facilitate communications relating to the proposed arms exports and opened a bank account in Hong Kong to receive and disburse funds related to the transactions. On a visit to New York in Feb. 2012, the defendants allegedly examined a Raven RQ-11b UAV and manuals relating to the RQ-4 Global Hawk UAV (provided by undercover FBI agents) that they allegedly intended to export to China. Shen and Chang were arrested shortly thereafter. The export investigation was conducted by the FBI, while ICE was responsible for a parallel investigation into the import of counterfeit goods from China involving other defendants.

***Trade Secrets to Competitors in China*** – On Dec. 10, 2014, Janice Kuang Capener, a citizen of China, was sentenced in the District of Utah to 90 days in prison, 24 months supervised release, \$100 special assessment, and a \$3,000 fine. Capener pleaded guilty on Sep. 11, 2014, to Count 3 of a second Superseding Indictment which charged the defendant with theft of trade secrets. Previously, on May 7, 2012, prosecutors unsealed an indictment charging Capener, Jun Luo and two companies, Sunhills International LLC, a California company established by Capener, and Zhejiang Hongchen Irrigation Equipment Co., LTD., with theft of trade secrets, wire fraud, and conspiracy to commit wire fraud in connection with the alleged theft of trade secrets from Orbit Irrigation Products, an irrigation company headquartered in Utah. According to court documents, Capener worked at Orbit from Jun. 2003, through Nov. 1, 2009, including serving as the chief of operations at Orbit's manufacturing plant in Ningbo, China. Capener allegedly stole Orbit's trade secrets relating to sales and pricing and used that information for herself and others to the detriment of Orbit. Capener also allegedly worked with Luo, Sunhills International and Zhejiang Hongchen Irrigation Equipment to devise a scheme to undermine Orbit's position in the marketplace using illegally obtained proprietary pricing information. Capener and Luo were arrested on May 4, 2012. On Aug. 29, 2012, all charges against Luo, also a citizen of China, were dismissed. Zhejiang Hongchen Irrigation Equipment Co., Ltd., a Chinese company under contract with Orbit, pleaded guilty to Counts 1-5 of the original indictment and was sentenced to 36 months of probation, and ordered to pay a fine of \$100,000 and restitution in the amount of \$300,000 for its role in a scheme to defraud and conspiracy to commit wire fraud. This case was investigated by the FBI.

***Firearms Parts to Russia*** – On Dec. 9, 2014, Viacheslav Zhukov was sentenced in the Southern District of Georgia to 51 months in prison, 3 years supervised release and \$100 special assessment following his plea of guilty on Dec. 5, 2014, for his role in illegally exporting firearm parts from the United States to Russia. An indictment was unsealed on Jun. 4, 2014, charging Zhukov with illegally exporting firearm parts from Savannah, Georgia to others in Russia. The indictment alleged that Zhukov, a Russian citizen and lawful permanent resident of the United States living in Savannah, GA, mailed multiple packages containing firearm magnifier scopes to Russia without first obtaining an export license from the United States Department of Commerce. Various firearm magnifier scopes are controlled under the Export Administration Regulations for crime control purposes and require a license from the United States Department of Commerce to export to Russia. The indictment further alleged that Zhukov misrepresented the contents of packages he mailed to Russia on the customs declarations forms presented to the United States Postal Service. This case was investigated by HSI, CBP, USPS, and the Savannah-Chatham Metropolitan Police Department.

***Embargo Violations by Alleged Arms Dealer*** – On Dec. 4, 2014, Richard Ammar Chichakli, an associate of international arms dealer Viktor Bout, was sentenced in the Southern District of New York to 60 months in prison, 2 years supervised release, \$900 special assessment and \$70,000 restitution. He was also ordered to forfeit \$1,732,756. Chichakli was arrested in Australia in Jan. 2013, and then extradited to the U.S. in May 2013. On Dec. 13, 2013, he was convicted by a jury of conspiring with Bout and others to violate the International Emergency Economic Powers Act ("IEEPA") by attempting to purchase commercial airplanes from American companies, in violation of U.S. sanctions. Chichakli, a citizen of Syria and the U.S., was also found guilty of money laundering conspiracy, wire fraud conspiracy, and six counts of wire fraud, in connection with the attempted aircraft purchases. According to evidence at trial and documents previously filed in Manhattan federal court, Chichakli conspired with Bout and others to violate IEEPA by engaging in prohibited business transactions with companies based in the United States. The focus of these transactions was the purchase of commercial airplanes for a company that Bout and Chichakli controlled, and the ferrying of those aircraft to Tajikistan. At the time of these unlawful transactions, both Chichakli and Bout had been designated by the U.S. Treasury Department as Specially Designated Nationals ("SDNs"), which meant that individuals and businesses in the United States were prohibited from engaging in financial transactions with them. Chichakli sought to evade these SDN sanctions by, among other things, concealing his identity and his SDN listing, and by concealing Bout's involvement in the airplane transactions. In connection with this fraudulent scheme, Chichakli helped to make a series of wire transfer payments, totaling more than \$1.7 million. These payments were sent from overseas bank accounts into accounts in the United States. Chichakli's co-conspirator, Bout, is currently serving a 25-year prison term as a result of his Nov. 2011, conviction in the Southern District of New York in connection with his conspiring to sell millions of dollars of weapons to a designated foreign terrorist organization. This case was investigated by the DEA-Special Operations Division.

***Military-Grade Weapons Exported Outside of the U.S.*** – On Nov. 21, 2014, Justin Gage Jangraw, a former U.S. Army officer who was once deployed to Iraq, was sentenced in the District of Columbia to 8 months in prison, one year of supervised release and \$125 special assessment. Previously, on Aug. 29, 2014, Jangraw pleaded guilty to violating the Arms Export Control Act by selling restricted items without a license. He also pleaded guilty to a separate charge stemming from his unauthorized removal and retention of classified documents that he obtained while he was in the Army. According to court documents, Jangraw operated an online business in Portland using the names "Heapeach" and "Sexyweapon.com". The business sold strictly regulated military-grade weapons parts and accessories to customers located worldwide.



From Nov. 2009, through Jan. 2011, Jangraw sold and exported from the United States a total of 287 Munitions List items – including riflescopes manufactured to military specifications - to international customers in 34 different foreign countries, generating more than \$12,000. Jangraw exported Munitions List parts and accessories even though he and his business never applied for or obtained a license to export defense articles from the United States. He did so with full knowledge of the licensing requirements. Following an undercover HSI investigation, HSI agents obtained a warrant to search Jangraw's residence, which was then in Portland. During the search, in Apr. 2011, agents seized four computers and electronic media, gun magazines, documents and products such as a weapon sight, gun rails, gun parts, and an AR-15 assault rifle. A subsequent review of images seized from Jangraw's laptop computer led to the discovery of classified material that included e-mails from Jangraw's work with the Army. The FBI was alerted and performed a follow-up search in Jul. 2011, that led to the discovery of additional material that Jangraw had removed, without authorization, from Iraq. He took the laptop with him to numerous foreign countries and accessed unprotected Wi-Fi networks with the laptop while it contained the classified documents. The hundreds of classified documents contained information on military plans, weapons systems or operations, and other subjects pertaining to national security. This case was investigated by ICE-HSI, FBI, and assisted the U.S. Central Command.

***Defense Articles Exported Outside of the U.S.*** – On Oct. 14, 2014, in the Middle District of Georgia, Robert J. Shubert, Sr., was sentenced to 78 months in prison following his earlier plea of guilty to one count each of conspiracy to violate and violation of the Arms Export Control Act as well as one count of possession of an unregistered firearm. The investigation in this case revealed that Mr. Shubert conspired with a foreign national between Jun. 2006, and Dec. 2011, to export defense articles to a foreign nation without the proper authority or license. He purchased the defense articles from various legitimate distributors and shipped them to a foreign nation at a considerable profit to himself. To facilitate the scheme, he also prepared false documents regarding the contents to be exported to his foreign co-conspirator. These acts formed the basis of the Arms Export Control Act violations. Additionally, search warrants executed on homes owned by Mr. Shubert in Warner Robins, Georgia, and in Wisconsin revealed more than 80 unregistered destructive devices, better known as pipe bombs. These resulted in the possession of an unregistered firearm count. The Court also imposed a fine of \$15,000.00 and ordered forfeiture of \$147,892.00. The Court prohibited Shubert from leaving the U.S. and ordered his passport be surrendered to the State Department, as well. The case was investigated by the Federal Bureau of Investigation and Homeland Security Investigations.

***High-Tech Night Vision Devices to Russia*** – On Oct. 9, 2014, Dmitry Ustinov, of Moscow, Russia, was sentenced in the District of Delaware to 18 months in prison and 3 years supervised release after a plea of guilty on Jul. 10, 2013, to conspiracy to export high-tech military technology, in violation of the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR). Previously, at the request of the U.S. government, Ustinov was arrested in Vilnius, Lithuania after entering that country from Russia. On Aug. 23, 2013, Lithuania extradited Ustinov to the United States. According to court documents, between Jul. 2010, and Apr. 2013, Ustinov, working with a supplier based in Virginia, caused or attempted to cause the export from the United States to Russia approximately seventeen different night vision devices and thermal imaging scopes, which are designated on the United States Munition List (USML) as defense articles, and are prohibited from export outside of the United States. The defense articles at issue include the Insight Mini Thermal Monoculars, D-740 night vision scopes, and Flir Tau 640 thermal imaging cameras, and are primarily used as weapons' mounted or helmet mounted night vision devices and in the case of the Flir Tau 640s, can even be mounted to fast moving vehicles or aircrafts, such as unmanned aerial vehicles. Given the sensitive nature of the defense articles at issue, Ustinov's scheme was designed to avoid detection by law

enforcement at each step in the process. First, Ustinov worked closely with a United States-based straw purchaser to conceal his involvement at the point of sale. Second, once a specific defense article was identified for purchase, Ustinov wired money to the straw purchaser to buy the defense article from front companies located in off-shore accounts in Cyprus. Finally, Ustinov also caused the packages containing USML defense articles to be falsely labeled so that customs officials from the United States and other countries would be less likely to search the package. Moreover, Ustinov also discussed using less traditional methods to obtain and export these night vision devices outside the United States, such as establishing a phony front company in the United States, and placing these high-tech devices inside chopped up car parts to conceal them from customs officials. At no time, however, did Ustinov ever apply for or receive a license to export these devices from the U.S. Department of State. This case was investigated by ICE-HSI.

***F-16 Military Parts to Venezuela*** – On Sep. 10, 2014, Ronald A. Dobek was sentenced in the Eastern District of Wisconsin to 84 months in prison, 3 years supervised release and \$100 special assessment. Previously, on Jun. 5, 2014, following a three-day jury trial, Ronald A. Dobek was convicted of conspiring to export and exporting F-16 military parts to the Venezuelan Air Force (“VAF”) without a license or authority from the U.S. Department of State. The jury returned guilty verdicts on all three counts of the indictment that charged Dobek with conspiring to violate U.S. export laws and unlawfully exporting F-16 parts to Venezuela on Dec. 29, 2007, and Dec. 6, 2008. The evidence presented at trial showed that Dobek conspired with a member of the VAF to supply the VAF with F-16 canopy seals for Venezuelan’s fleet of F-16 military jets. The evidence showed that Dobek exchanged numerous emails with a member of the VAF in which they discussed obtaining the F-16 canopy seals and the need to keep their operation secret. Dobek took other steps to conceal his illegal activity, including misidentifying the shipments as “t-molding” on shipping documents. As a result, Dobek sent shipments of F-16 canopy seals to a member of the VAF in Venezuela on or about Dec. 29, 2007, and Dec. 6, 2008. This case was investigated by the Federal Bureau of Investigation, Department of Homeland Security, Homeland Security Investigations, and the Department of Defense, Office of Inspector General.

***DuPont Trade Secrets to China*** – On Aug. 26, 2014, Robert J. Maegerle was sentenced in the Northern District of California to serve 30 months’ imprisonment, pay \$367,679 in restitution and a \$400 special assessment. On Jul. 10, 2014, Walter Lian-Heen Liew and his company, USA Performance Technology, Inc. (USAPTI), were both sentenced. Liew was sentenced to serve 15 years’ imprisonment, forfeit \$27.8 million in illegal profits, and pay \$511,487.82 in restitution and a \$2,000 special assessment. USAPTI was sentenced to 5 years’ probation and to pay a fine of \$18.9 million and a \$3,600 special assessment. Previously, on Mar. 5, 2014, Liew, his company, USAPTI, and Maegerle were found guilty of economic espionage, theft of trade secrets, bankruptcy fraud, tax evasion, and obstruction of justice for their roles in a long-running effort to obtain U.S. trade secrets for the benefit of companies controlled by the government of the People's Republic of China (PRC). The jury found that Liew, USAPTI, and Maegerle conspired to steal trade secrets from E.I. du Pont de Nemours & Company (DuPont) regarding their chloride-route titanium dioxide production technology and sold those secrets for large sums of money to state-owned companies of the PRC. The purpose of their conspiracy was to help those companies develop large-scale chloride-route titanium dioxide production capability in the PRC, including a planned 100,000-ton titanium dioxide factory in Chongqing. This case marked the first jury conviction for economic espionage (18 U.S.C. Section 1831). Liew was convicted of conspiracy to commit economic espionage, conspiracy to commit theft of trade secrets, attempted economic espionage, attempted theft of trade secrets, possession of trade secrets, conveying trade secrets, conspiracy to obstruct justice, witness tampering, conspiracy to tamper with evidence, false statements, filing false tax returns for USAPTI and Performance Group, a predecessor company to USAPTI, and false statements and oaths in bankruptcy proceedings.

Liew was an owner and president of USAPTI, a company headquartered in Oakland, Calif., that offered consulting services. USAPTI was found guilty of conspiracy to commit economic espionage, conspiracy to commit theft of trade secrets, attempted economic espionage, attempted theft of trade secrets, possession of trade secrets, conveying trade secrets, and conspiracy to obstruct justice. Evidence at trial showed that in the 1990s, Liew met with the government of the PRC and was informed that the PRC had prioritized the development of chloride-route titanium dioxide (TiO<sub>2</sub>) technology. TiO<sub>2</sub> is a commercially valuable white pigment with numerous uses, including coloring paint, plastics, and paper. DuPont's TiO<sub>2</sub> chloride-route process also produces titanium tetrachloride, a material with military and aerospace uses. Liew was aware that DuPont had developed industry leading TiO<sub>2</sub> technology over many years of research and development and assembled a team of former DuPont employees, including Maegerle, to assist him in his efforts to convey DuPont's TiO<sub>2</sub> technology to entities in the PRC. Liew executed contracts with state-owned entities of the PRC for chloride-route TiO<sub>2</sub> projects that relied on the transfer of illegally obtained DuPont technology. Liew, Maegerle, and USAPTI obtained and sold DuPont's TiO<sub>2</sub> trade secret to the Pangang Group companies for more than \$20 million. Maegerle was convicted of conspiracy to commit theft of trade secrets, attempted theft of trade secrets, conveying trade secrets, and conspiracy to obstruct justice. Evidence at trial showed that Maegerle was employed by DuPont as an engineer from 1956 to 1991 where he had developed detailed knowledge of DuPont's TiO<sub>2</sub> technology and expertise in building TiO<sub>2</sub> production lines. He also had access to DuPont TiO<sub>2</sub> trade secrets, including specific information regarding DuPont's TiO<sub>2</sub> facility at Kuan Yin, Taiwan. He provided these trade secrets to Liew and USAPTI in furtherance of their contracts with state-owned companies of the PRC for chloride-route TiO<sub>2</sub> projects. Liew, Maegerle, and USAPTI's obstructing justice convictions stem from causing an answer to be filed in a federal civil lawsuit in which they falsely claimed that no information from DuPont's Kuan Yin plant was used in the USAPTI designs for the development of TiO<sub>2</sub> manufacturing facilities. Liew's witness tampering conviction stems from his efforts to influence a co-defendant's testimony in the civil lawsuit. The jury also convicted Liew of conspiring with his wife, Christina Hong Qiao Liew (aka Qiao Hong), who was charged in the second superseding indictment, to mislead the FBI by corruptly concealing records, documents, and other objects during the FBI's investigation into their criminal activity. Christina Liew, as co-owner of USAPTI, entered into contracts worth in excess of \$20 million to convey TiO<sub>2</sub> trade secret technology to Pangang Group companies. Liew and his wife received millions of dollars of proceeds from these contracts. The proceeds were wired through the United States, Singapore, and ultimately back into several bank accounts in the PRC in the names of relatives of Christina Liew. DuPont is a company based in Wilmington, Del., that manufactures a wide variety of products, including TiO<sub>2</sub>. DuPont invented the chloride-route process for manufacturing TiO<sub>2</sub> in the late-1940s and since then has invested heavily in research and development to improve that production process. The global titanium dioxide market has been valued at roughly \$12 billion per year, and DuPont has the largest share of that market. The chloride-route process is cleaner, more efficient, and produces a higher-quality product than the sulfate-route process prevalent in the PRC. The object of the defendants' conspiracy was to convey DuPont's secret chloride-route technology to the PRC companies for the purpose of building modern TiO<sub>2</sub> production facilities in the PRC without investing in time-consuming, costly research and development. The second superseding indictment charged Christina Liew, Tze Chao (aka Zhao Zhi) and Hou Shengdong each with conspiracy to commit economic espionage. Christina Liew was also charged with conspiracy to commit theft of trade secrets, attempted theft of trade secrets, possession of trade secrets, witness tampering, conspiracy to tamper with evidence, and false statements. The charges against Christina Liew were severed from those against Walter Liew, Maegerle, and USAPTI. On May 6, 2015, Christina Liew pleaded guilty to conspiracy to tamper with evidence and was sentenced on Oct. 10, 2015, to 3 years' probation, \$100 special assessment, \$25,000 fine and \$6,029,391 restitution. Chao, a former DuPont employee, pleaded guilty to conspiracy to commit

economic espionage on Mar. 1, 2012. Shengdong, the Vice Director of the Chloride Process TiO<sub>2</sub> Project Department for the Pangang Group, was also charged with conspiracy to commit theft of trade secrets and attempted economic espionage. He is currently a fugitive. Charges of conspiracy to commit economic espionage, conspiracy to commit theft of trade secrets, and attempted economic espionage are also pending against the four PRC state-owned companies charged in the second superseding indictment. This case was investigated by the FBI and the IRS Criminal Investigation.

***Electronics to UAE and Africa*** – On Aug. 13, 2014, R&A International Logistics (R&A), a privately-owned freight-forwarding company, was sentenced in the Eastern District of New York to 2 years' probation, \$4,000 special assessment and \$100,000 fine. Rukhsana Kadri, the owner and president of R&A, was sentenced to 3 years' probation, \$100 special assessment, \$30,000 fine, and ordered to forfeit \$125,262. Previously, on Dec. 9, 2013, during her initial appearance, Kadri pleaded guilty to falsifying Shipper's Export Declarations (SEDs) in connection with the international shipment of hundreds of Hewlett Packard computers, in violation of 13 U.S.C. 305. According to court documents, Kadri was responsible for the day-to-day operations of R&A's New York City Office. In addition, she supervised R&A's compliance with international export regulations. Between Jan. 2008, and Apr. 2012, R&A and Kadri repeatedly filed false SEDs relating to the shipment of electronics from the United States to the United Arab Emirates, Zimbabwe and Kenya.

***Pressure Transducers with Nuclear Applications to China and Elsewhere*** – On Jul. 24, 2014, in the District of Massachusetts, Qiang Hu aka Johnson Hu, a Chinese national and resident of Shanghai, was sentenced to 34 months in federal prison and \$100 special assessment. Hu pleaded guilty on Oct. 16, 2013, for his role in a conspiracy scheme to export dual-use pressure transducers from the United States to China. Previously, on Jun. 13, 2012, a grand jury returned an indictment charging Hu with conspiracy to illegally export from the United States to China and elsewhere dual-use pressure transducers, in violation of the International Emergency Economic Powers Act (IEEPA). Pursuant to a criminal complaint, Hu was arrested on May 22, 2012, after he arrived in Massachusetts for a business meeting. According to the indictment, the pressure transducers in question, manufactured by MKS Instruments headquartered in Andover, Mass., are controlled for export by the Commerce Department because they can be used in gas centrifuges to enrich uranium and produce weapons-grade uranium. Specifically, they can be used to measure gas pressure of uranium hexafluoride in centrifuge cascades. The indictment claims that Hu worked as a sales manager for a subsidiary of MKS Instruments in Shanghai, where he has been employed since 2008. Hu and his co-conspirators allegedly caused thousands of MKS export-controlled pressure transducers, worth more than \$6.5 million, to be illegally exported from the United States to unauthorized end-users in China and elsewhere using export licenses fraudulently obtained from the Department of Commerce. The indictment alleged that Hu and his co-conspirators used two primary means of deception to export the pressure transducers. First, the conspirators used licenses issued to legitimate MKS business customers to export the pressure transducers to China, and then caused the parts to be delivered to other end-users who were not themselves named on the export licenses or authorized to receive the parts. Second, the conspirators obtained export licenses in the name of a front company and then used these fraudulently obtained licenses to export the parts to China, where they were delivered to the actual end-users. MKS is not a target of the federal investigation into these matters. This investigation was conducted by FBI, ICE, and BIS.

***Information Technology Services and Support to Iran*** – On Jul. 17, 2014, Randy Dale Barber was sentenced in the Middle District of Florida to 60 months' probation for conspiracy to commit mail fraud. Barber was also ordered to forfeit \$413,106 and to pay restitution to Hitachi Data

Systems (HDS) in the amount of \$37,921.20. Barber previously pleaded guilty on Feb. 28, 2014, to a superseding indictment. On Apr. 30, 2014, Barber's co-defendants, John Alexander Talley and his company, Tallyho Peripherals, Inc. d/b/a Enterprise Solutions Systems, were sentenced after pleading guilty on Sep. 17, 2013, to conspiracy to violate the International Emergency Economic Powers Act and the Iranian Transaction Regulations. Talley was sentenced to 30 months in federal prison, 36 months supervised release and \$100 special assessment. Tallyho Peripherals, Inc., was sentenced to 12 months' probation and \$400 special assessment. According to plea agreements, from approximately 2009 to Sep. 2012, Barber, Talley and his company conspired with others to unlawfully export sophisticated enterprise level computer equipment from the United States to Iran, and to provide computer IT support services for the equipment, all in violation of the United States embargo. Talley's role was to provide training and computer IT support to ensure that the computer equipment operated in Iran. In an effort to conceal their activities, the conspirators in the United States caused shipments of the computers and related equipment, as well as the payments for same, to travel to and from the United States and Iran through the United Arab Emirates. Similarly, payments for Talley's support services were transmitted through the United Arab Emirates. On Sep. 12, 2013, two Iranian nationals, Mahmood Akbari a/k/a John Wassermann and Reza Hajigholamali, and three United Arab Emirate "front" companies, Patco Group Ltd., Managed Systems and Services (FZC), and TGO General Trading LLC a/k/a Three Green Orbit, were indicted in connection with the same conspiracy to violate the Iranian Embargo. Those parties were charged with conspiracy to violate the International Emergency Economic Powers Act and the Iranian Transactions and Sanctions Regulations, and a conspiracy to commit international money laundering. On Jul. 11, 2012, co-conspirator Mohammad Reza "Ray" Hajian and three of his companies, RH International LLC, Nexiant LLC, and P & P Computers LLC, pleaded guilty to conspiracy to violate the International Emergency Economic Powers Act and the Iranian Transactions and Sanctions Regulations. On Oct. 18, 2012, Hajian was sentenced to 4 years in federal prison and ordered to forfeit \$10 million. This investigation was conducted by ICE and DOC.

***Military Software Used For China's First Modern Attack Helicopter*** – On Jul. 14, 2014, in the District of Connecticut, the court signed an order dismissing the criminal information against United Technologies Corporation (UTC) and Hamilton Sundstrand Corporation (HSC) and dismissing counts three of the information against Pratt & Whitney Canada Corp. (PWC). Previously, on Jun. 28, 2012, PWC, a Canadian subsidiary of Connecticut-based defense contractor UTC, pleaded guilty to violating the Arms Export Control Act and making false statements in connection with its illegal export to China of U.S.-origin military software that was used in the development of China's first modern military attack helicopter, the Z-10. In addition, UTC, its U.S.-based subsidiary HSC, and PWC all agreed to pay more than \$75 million as part of a global settlement with the Justice Department and the State Department in connection with various export violations, including those related to the Z-10, and for making false and belated disclosures to the U.S. government about the illegal exports for the Z-10. A three-count criminal information was filed against the companies. Count one charged PWC with violating the Arms Export Control Act for the illegal export of defense articles to China for the Z-10 helicopter. Specifically, in 2002 and 2003 PWC knowingly and willfully caused HSC military software used to test and operate PWC engines to be exported to China for the Z-10 without any U.S. export license. PWC knew from the start of the Z-10 project in 2000 that the Chinese were developing an attack helicopter and that supplying it with U.S.-origin components would be illegal. According to court documents, PWC's illegal conduct was driven by profit. PWC anticipated that its work on the Z-10 attack helicopter in China would open the door to a far more lucrative civilian helicopter market in China potentially worth as much as \$2 billion to PWC. Count two of the information charged PWC, UTC, and HSC with making false statements about these illegal exports to the State Department in their belated disclosures, which did not begin until 2006.

Count three charged PWC and HSC for their failure to timely inform the State Department of the unlawful export of defense articles to China, an embargoed nation, as required by U.S. export regulations. This is the first case in which the provisions in count three have been enforced criminally. While PWC pleaded guilty to counts one and two, prosecution of PWC, UTC, and HSC on the other charges was deferred for two years, provided that the companies abided by the terms of a deferred prosecution agreement with the Justice Department. In addition to the resolution of the criminal charges, as part of a global settlement, UTC also resolved over 500 additional administrative charges with the State Department. Those charges involved more than 800 exports in violation of the Arms Export Control Act from the mid-1990s to 2011. In connection with the global settlement with the Justice and State Departments, PWC, UTC, and HSC agreed to pay more than \$75 million in penalties, subject themselves to independent monitoring for several years, and be required to comply with an extensive training and remedial action program to strengthen their export compliance. This investigation was conducted by ICE, DCIS, FBI, Commerce and the State Department.

***Prohibited Investments in Iran*** – On Jun. 20, 2014, former Tennessee Valley Authority (TVA) vice president, Masoud Bajestani, of Chattanooga, Tenn., was sentenced in the Eastern District of Tennessee to 2 years’ probation, \$300 special assessment and the forfeiture of \$600,000. On Sep. 4, 2013, Bajestani pleaded guilty to violating the International Emergency Economic Powers Act and filing false tax returns. On Feb. 4, 2013, agents arrested Bajestani as he arrived at the Atlanta airport on a flight from Dubai. Bajestani was charged by superseding indictment in the Eastern District of Tennessee with violating the International Emergency Economic Powers Act, making false statements to the TVA, international money laundering, filing false tax returns and failure to file reports of foreign bank accounts. According to the superseding indictment, Bajestani filed a false document with TVA in order to withdraw \$1,500,000 from his deferred compensation account when he was employed as a vice president at the Watts Bar Unit II nuclear power plant during its construction phase. Bajestani then conspired with others and sent \$600,000 of those funds to Iran for financial investment purposes, without authorization from the U.S. Office of Foreign Assets Control. The case was investigated by ICE, IRS, the TVA Office of Inspector General, and the FBI.

***Aircraft Parts, Technologies and Services to Iran, Sudan and Burma*** – On Jun. 5, 2014, in the District of Columbia, Fokker Services B.V., a Dutch aerospace services provider, agreed to forfeit \$10.5 million to the United States for conspiring to violate the International Emergency Economic Powers Act (IEEPA) by engaging in illegal transactions involving the export of aircraft parts, technologies, and services to customers in Iran, Sudan, and Burma. The company also entered into a parallel settlement agreement with the Commerce Department’s Bureau of Industry and Security (BIS) and the Treasury Department’s Office of Foreign Assets Control (OFAC). A criminal Information was filed on Jun. 5, 2014, charging Fokker Services B.V. with one count of knowingly and willfully conspiring to violate the IEEPA, in violation of 18 U.S.C. § 371. Fokker Services waived the requirement of being charged by way of federal Indictment, agreed to the filing of the Information, and accepted responsibility for its criminal conduct and that of its employees. In addition, as part of the deferred prosecution agreement reached, Fokker Services agreed to forfeit \$10.5 million within five days of the approval of the agreement by the Court. According to court documents, starting on or about late 2005 and ending on or about late 2010, Fokker Services violated U.S. laws by engaging in illegal transactions involving the export and re-export of aircraft parts, technology, and services to customers located in U.S.-sanctioned countries, specifically, Iran, Sudan, and Burma. Throughout this period, Fokker Services knowingly and willfully engaged in this criminal conduct, fully aware of the application of U.S. export laws, an issue which was repeatedly raised internally with the company’s management. In Jun. 2010, Fokker Services made a disclosure of potential violations to BIS and OFAC in which

the company acknowledged and accepted responsibility for its unlawful conduct. Fokker Services' criminal conduct included knowingly initiating, either directly or indirectly, 1,153 shipments of aircraft spare, repaired, or exchanged parts with a U.S. nexus to Fokker Services' customers in Iran, Sudan, or Burma. Among those illegal transactions were 99 transactions involving Fokker Services' customer, Iran Air, which was the subject of a special order from the U.S. Department of Commerce prohibiting Fokker or any third party from exporting U.S.-origin commodities to Iran Air or providing services to Iran Air. Fokker Services' gross revenue for the shipments in violation of U.S. export control laws amounted to approximately \$21 million. According to court documents, Fokker Services used a number of schemes to evade U.S. sanctions and export laws while continuing its business with customers located in U.S.-sanctioned countries and specifically designed to continue the company's profit earnings in the sanctioned countries' markets. Internally, Fokker Services described these as "work-arounds." Some examples of the work-arounds used by Fokker Services and its employees include the following: deliberately withholding aircraft tail numbers to U.S.-based repair shops, providing false tail numbers to U.S. and U.K. companies and repair shops, and stating that the parts submitted for repair by U.S.-repair shops were to be used as "stock" parts. Fokker Services engaged in this conduct as an intentional effort to conceal the company's affiliation with customers located in U.S. sanctioned countries. On one occasion, Fokker Services provided a U.S. aerospace company with a work order that falsely represented that the aircraft part belonged to an airplane owned by a Portuguese airline when, in reality, the part actually belonged to an Iran Air aircraft. The U.S. aerospace company fixed the part and returned it to Fokker Services, who then shipped the part to Iran. Other work-arounds were designed by Fokker Services to further the company's efforts of continuing to engage in transactions in violation of U.S. export laws while also avoiding detection of U.S. authorities, for example, the company constructed and constantly updated a chart it called "the black list" that tracked which U.S. companies were more vigilant about export controls, and directed its business to those U.S. companies that were not on "the black list." The company also deleted references to Iran in materials sent to its U.S. subsidiaries and U.S. repair shops. It changed an internal database that tracked parts to delete fields related to ultimate end-user information, and directed employees to hide activities and documents related to Iranian transactions when inspectors from the U.S. Federal Aviation Administration audited Fokker Services' Dutch warehouse. According to court documents, this conduct occurred in various business units within Fokker Services and certain policies and practices in furtherance of Fokker Services' criminal conduct were carried out with the knowledge and approval of the company's senior corporate managers, as well as with the knowledge of the company's Legal and Export Compliance departments. The Justice Department's investigation of Fokker Services arose out of the company's disclosure of potential violations to BIS and OFAC in Jun. 2010. In its initial disclosure, Fokker Services acknowledged and accepted responsibility for its unlawful conduct. Over the next two-and-a-half years, Fokker Services conducted a vast internal investigation through outside counsel and disclosed additional violations of U.S. export laws. Since the submission of its 2010 disclosure to U.S. authorities, Fokker Services has taken steps to enhance and optimize its sanctions compliance programs, including stopping all new business with customers located in U.S.-sanctioned countries; launching an employee disciplinary review to investigate and address the conduct of all employees, including senior management, who were involved in the apparent violations; adopting a new Export Compliance Program; and terminating relationships with sanctioned banks and closing its Iranian representative office and branch. This investigation was conducted by the FBI, Department of Commerce-BIS Office of Export Enforcement; ICE-HSI; and the New Haven, Connecticut office of the Defense Criminal Investigative Service.

***Electronics Used in Military Radar & Electronic Warfare to China*** – On Apr. 30, 2014, Yufeng Wei, a Chinese national, was re-sentenced to 23 months in prison, 2 years of supervised released,

and \$1100 special assessment. Previously, on Sep. 10, 2013, Wei's now ex-husband Zhen Zhou Wu, also a Chinese national, was re-sentenced to 84 months in prison, 2 years of supervised release, \$1700 special assessment, and ordered to pay a \$15,000 fine. Wei and Wu were re-sentenced for conspiring over a 10-year-period to illegally export military and sophisticated electronics used in military phased array radar, electronic warfare, and missile systems to the People's Republic of China (PRC) and illegally exporting sensitive electronic components to the PRC between 2004 and 2007, in violation of the Export Administration Regulations. After serving their convictions, both Wu and Wei, a Lawful Permanent Resident, will be subject to deportation to the PRC. On Mar. 19, 2013, the U.S. Court of Appeals for the First Circuit affirmed both Wei and Wu's convictions on export violation charges for which a jury convicted them after a six-week trial in May 2010. The First Circuit vacated two counts of the convictions that charged Wei and Wu with illegally exporting parts designated on the United States Munitions List because it held that the jury instructions given were constitutionally inadequate. However, the First Circuit observed that "from 1996 until 2008, Wei and Wu shipped tens of millions of dollars' worth of sophisticated electronic components from the United States to China with little regard for whether the parts that they sold were export-controlled." Further, the First Circuit found that Wu's company "specifically pursued military customers; and Wu promoted himself as both an exporter of military supplies and an export compliance expert." Lastly, the First Circuit determined that "Wu and Wei repeatedly attempted to disguise the fact that they were exporting to China and that they lacked the necessary licenses to do so." Because two counts of both Wei and Wu's convictions were vacated, the case was remanded for re-sentencing hearings. Wei and Wu were originally sentenced in 2011. On Jan. 27, 2011, in the District of Massachusetts, Wei was sentenced to 36 months in prison; while on Jan. 26, 2011, Wu was sentenced to 97 months in prison. Their company, Chitron Electronics, Inc., was fined \$15.5 million. Wei, Wu and Chitron Electronics, Inc. were convicted at trial on May 17, 2010. As proven at trial, defendants illegally exported military electronic components to China through Hong Kong. The defendants also illegally exported Commerce Department-controlled electronics components to China with military applications such as electronic warfare, military radar, and satellite communications systems. Wu founded and controlled Chitron, with headquarters in Shenzhen, China and a U.S. office located in Waltham, Mass., where defendant Wei served as Manager. Wu and Chitron sold electronics from the U.S. to Chinese military factories and military research institutes, including numerous institutes of the China Electronics Technology Group Corporation, which is responsible for the procurement, development and manufacture of electronics for the Chinese military. Since as early as 2002, Wu referred to Chinese military entities as Chitron's major customer and employed an engineer at Chitron's Shenzhen office to work with Chinese military customers. By 2007, 25% of Chitron's sales were to Chinese military entities. Shenzhen Chitron Electronics Company Limited, Wu's Chinese company through which U.S. electronics were delivered to the Chinese military and other end-users, was also indicted. On Feb. 9, 2011, Chitron-Shenzhen received a fine of \$1.9 million for refusing to appear for trial. On Jul. 22, 2010, co-defendant Bo Li, aka Eric Lee, pleaded guilty and was sentenced to time served for making false statements on shipping documents. The case was investigated by BIS, ICE, FBI, and DCIS.

***Nuclear-Related Dual-Use Equipment to Iran*** – On Apr. 29, 2014, Li Fangwei, who is more commonly known by his alias "Karl Lee," was charged in the Southern District of New York with violating the International Emergency Economic Powers Act ("IEEPA") by using United States-based financial institutions to engage in millions of dollars of U.S. dollar transactions in violation of economic sanctions that prohibited such financial transactions. In addition, Fangwei is also charged with conspiring to commit wire fraud and bank fraud, a money laundering conspiracy, two separate violations of IEEPA, and two separate substantive counts of wire fraud, in connection with such illicit transactions. Fangwei, a national of the People's Republic of



China, is a fugitive. According to the Superseding Indictment, Fangwei controls a large network of industrial companies based in eastern China, one of which is LIMMT Economic and Trade Company, Ltd. (“LIMMT”). Over the years, Fangwei’s companies have done millions of dollars in business with Iran. This business has included selling to Iranian entities various metallurgical goods and related components that are banned for transfer to Iran by, among others, the United Nations, because the items are controlled by the Nuclear Supplier’s Group (a multinational group that maintains “control lists,” which identify nuclear-related dual-use equipment, material, and technology). Fangwei has been, among other things, a long-time supplier to Iran’s Defense Industries Organization and Iran’s Aerospace Industries Organization. In addition, Fangwei has been a principal contributor to Iran’s ballistic missile program through China-based entities that have been sanctioned by the United States. In light of his supply of restricted items to Iran, the United States has imposed targeted sanctions on both Fangwei and LIMMT. Specifically, the United States Department of the Treasury’s Office of Foreign Asset Controls (“OFAC”) publicly added LIMMT (in 2006) and Fangwei (in 2009) to its List of Specially Designated Nationals and Blocked Persons (the “SDN List”). By virtue of their inclusion on the SDN List, Fangwei and LIMMT were effectively precluded from conducting any business within the United States without first obtaining a license or authorization from OFAC. Neither Fangwei nor LIMMT has sought such a license or authorization. The above-referenced restrictions have forced Fangwei to operate much of his business covertly. In response to United States sanctions, Fangwei has built an outsized network of China-based front companies – to conceal his continuing participation, and LIMMT’s continuing participation, in sanctioned activities. During the period from 2006 through 2014, Fangwei used front companies to engage in more than 165 separate U.S. dollar transactions, with a total value in excess of approximately \$8.5 million. Included in those illicit transactions have been transactions involving sales to U.S. companies, sales of merchandise by Fangwei to Iran-based companies utilizing the U.S. financial system, as well as attempts to acquire on behalf of Iran-based entities so-called “dual use” items from the United States, China, and other countries that could be used in the production of weapons of mass destruction and/or devices used to deliver weapons of mass destruction. The U.S. Attorney’s Office and the FBI announced the seizure of over \$6,895,000 in funds attributable to the Fangwei front companies, and the filing of a civil complaint seeking the forfeiture of those funds to the United States. The seized funds are substitutes for money held by Fangwei’s front companies at banks in China, and were seized from accounts at U.S. banks held in the name of foreign banks used by these front companies to conduct U.S. currency transactions. The funds were seized pursuant to seizure warrants issued on Dec. 18, 2013, and Apr. 25, 2014. The \$6,895,000 represents funds used by the Fangwei front companies to engage in transactions that violate the U.S. sanctions laws and thus are subject to forfeiture. There are no allegations of wrongdoing by the U.S. or foreign banks that maintain these accounts. Because the funds used in those transactions are held in banks overseas, the United States is unable to seize the funds directly. This case was investigated by the Federal Bureau of Investigation, Department of State, Department of Treasury, and the Department of Commerce.

***Military Aircraft Engines to Venezuela*** – On Apr. 28, 2014, Roy Wayne Roby pleaded guilty and was sentenced in the District of Arizona to 18 months in federal prison, 3 years of supervised release, and \$100 special assessment for his role in a conspiracy to violate the Arms Export Control Act. According to court documents, Roby was part of a Venezuelan air force team that negotiated with Mesa-based Marsh Aviation between Nov. 2005, and Feb. 2008, to refurbish 18 T-76 aircraft engines for use by the Venezuelan air force, under the guise that the engines were meant for civilian use. T-76 engines are a designated item on the U.S. Munitions List, which, under the Arms Export Control Act, makes it illegal for these engines to be exported without a license or written authorization from the Department of State. The T-76 aircraft engine was designed for the OV-10 Bronco Aircraft, a light armed reconnaissance aircraft specifically suited

for counter-insurgency missions. Roby and codefendants Guiseppe Luciano Menegazzo-Carrasquel, a dual Venezuelan and Italian citizen, and Oscar Rafael Colmenarez-Vellalobos were indicted on arms export charges in Oct. 2010. Roby was arrested in Florida on Sep. 4, 2013. Menegazzo-Carrasquel, a Venezuelan air force colonel, was arrested in Sep. 2012, after he arrived in Houston on a flight from Caracas, using his Italian passport. On Jun. 3, 2013, Menegazzo-Carrasquel pleaded guilty and on Aug. 19, 2013, he was sentenced to 19 months in federal prison and 3 years of supervision. Indicted in a separate case, Floyd D. Stilwell, former president of Marsh Aviation, was also charged in the scheme. Stilwell pleaded guilty on Oct. 29, 2012, to conspiracy to violate the Arms Export Control Act and was sentenced on May 13 to a \$250,000 fine and 5 years of probation. The case was investigated by ICE, DCIS and the FBI.

***Missiles, Aviation Equipment and Submarine Design Information to Terrorist Organization –***

On Mar. 25, 2014, Piratheepan Nadarajah, an alleged operative of the Liberation Tigers of Tamil Eelam (LTTE), a designated terrorist organization known as the “Tamil Tigers”, was sentenced in the Eastern District of New York to 24 months in federal prison, 3 years supervised release and \$100 special assessment. On Oct. 8, 2013, Nadarajah pleaded guilty to attempting to provide material support to a foreign terrorist organization and conspiracy to acquire anti-aircraft missiles. Previously, on Dec. 27, 2012, Nadarajah and Suresh Sriskandarajah made their initial court appearances in the Eastern District of New York after being extradited from Canada. Nadarajah is charged by superseding indictment with conspiring and attempting to acquire \$1 million worth of anti-aircraft missiles, missile launchers and other military equipment, and conspiring and attempting to provide material support to the LTTE. Sriskandarajah is charged under a separate indictment with conspiring to provide material support to the LTTE and dealing in the property of a specially designated terrorist group. According to court filings, between Jul. 1, 2006, and Aug. 19, 2006, Nadarajah and several co-conspirators engaged in negotiations with an undercover FBI agent to purchase and export \$1 million worth of high-powered weapons and military equipment for the LTTE, including 20 SA-18 heat-seeking, surface-to-air, anti-aircraft missiles, 10 missile launchers and 500 AK-47s. Nadarajah and his associates attempted to acquire these weapons at the direction of senior LTTE leadership in Sri Lanka, including Pottu Amman, then the LTTE's chief of intelligence and procurement and the top deputy to then LTTE leader Velupillai Prabhakaran. The anti-aircraft weapons were to be used by the LTTE to shoot down Kfir aircraft used by the Sri Lankan military. Co-conspirators Sahilal Sabaratnam, Thiruthanikan Thanigasalam, and Nadarasa Yogarasa were each sentenced in Sep. 2011. Sabaratnam was sentenced on Sep. 23, 2011, to 25 years' imprisonment, 5 years supervised release, and \$400 special assessment. Yogarasa was sentenced on Sep. 23, 2011, to 14 years' imprisonment, three years supervised release, and \$200 special assessment. Thanigasalam was sentenced on Sep. 26, 2011, to 25 years' imprisonment, 5 years supervised release and \$400 special assessment. Sathajhan Sarachandran was sentenced on Sep. 26, 2011, to 26 months' imprisonment, 5 years supervised release, and \$500 special assessment. This investigation was conducted by the Newark and New York Divisions of the FBI's Joint Terrorism Task Force.

***Restricted Electronics to China –*** On Mar. 23, 2014, General Technology Systems Integration, Inc. (GTSI) was sentenced in the Central District of California to 5 years' probation and a special assessment of \$400. On October 10, 2010, an indictment was returned charging York Yuan Chang, also known as David Zhang, and his wife, Leping Huang, with conspiring to export restricted electronics technology to the People's Republic of China (PRC) without first obtaining a license, in violation of 50 U.S.C. § 1705; and making false statements, in violation of 18 U.S.C. § 1001. According to court documents, the defendants were the owners of GTSI, a company based in California. GTSI entered into contracts with the 24th Research Institute of the China Electronics Technology Corporation Group in the PRC to design and transfer to the PRC technology for the development of two types of high-performance analog-to-digital converters

(ADCs). The defendants hired two engineers to design the technology and provided training to individuals in the PRC. Twice in 2009, U.S. Customs and Border Protection officials stopped the engineers upon their return to the United States and found computer files and documents indicating illegal technology transfer involving GTSI and the PRC. According to the complaint, Chang and Huang sought to cover up the project after authorities contacted the engineers. The ADCs that the defendants attempted to export to the PRC are subject to export controls for national security and anti-terrorism reasons. This investigation was conducted by the FBI, BIS, ICE, IRS and DCIS.

***Ammunition and Night Vision Goggles to Mexico*** – On Mar. 20, 2014, in the Western District of Texas, Oliver Bres-Carranza was sentenced to 51 months in federal prison after pleading guilty in Oct. 2013, for his role in a scheme to smuggle defense articles into the Republic of Mexico. On Jan. 15, 2014, Erik Alan Garza was sentenced to 44 months in federal prison and fined \$3,000 for his role in the smuggling scheme. Garza, Bres-Carranza and Rolando Tamayo were charged in a Jun. 2012, indictment with multiple counts of aiding and abetting the smuggling of goods from the United States. According to the indictment, between Jun. 19, 2010, and Feb. 17, 2012, Garza and his accomplice, Tamayo, illegally attempted to smuggle defense articles into the Republic of Mexico from the United States. Those items included night vision monocular goggles, a thermal goggle, 400 sets of AR-15 front and rear flip-up tactical sights, approximately 5,000 high-capacity assault rifle magazines and approximately 6,000 rounds of ammunition, including 100 rounds of .50 caliber ammunition. Tamayo remains a fugitive. This case was investigated by ICE and ATF.

***Hazardous Materials to Saudi Arabia*** - On Feb. 21, 2014, Hasan Ibrahim was sentenced in the Northern District of California to 30 days' imprisonment, 3 years of supervised release, and a \$2,200 special assessment. Previously, on Jul. 3, 2013, Ibrahim was convicted by a federal jury of attempting to place destructive substances on an airplane. The jury found that the defendant willfully intended to place 9 different hazardous materials on a Lufthansa passenger airplane bound for Frankfurt, Germany. The hazardous materials were ultimately destined for Jeddah, Saudi Arabia. In related charges, the jury convicted Ibrahim of failing to properly label the packages containing the hazardous materials and failing to complete the requisite shipping papers as required by the Department of Transportation. On Nov. 2, 2011, a grand jury returned an indictment charging MEDCHEM Corporation and its owner Hasan Ibrahim with two counts of attempted placement of destructive substance on an aircraft, one count of transportation of hazardous materials without shipping papers, nine counts of transportation of hazardous materials without labels, one count of failure to file export information, one count of attempted smuggling of goods, and one count of attempted smuggling of goods. The charges in the indictment stem from MEDCHEM, located in South San Francisco, exporting chemicals (including hazardous materials), medical equipment, and diagnostics to Constant Trading Activity ("CTA"), a business in Saudi Arabia. Ibrahim was the owner and president of MEDCHEM until one of his sons became involved in MEDCHEM prior to Jun. 2010. Ibrahim was MEDCHEM's sole employee. Ibrahim was also a founder of CTA and served as CTA's vice president. According to the indictment, Ibrahim caused a shipment consisting of five pallets containing sixty-four boxes to be delivered to a freight forwarder for export to Saudi Arabia. None of the boxes were labeled as containing hazardous material. The shipment contained over 25 separate chemicals designated as hazardous materials under the Hazardous Materials Regulations. Two of the hazardous materials - Sulfuryl Chloride (classified as a corrosive) and Chloroacetonitrile (classified as poisonous material, with a subsidiary hazard that it is a flammable and combustible liquid) - were poisonous by inhalation and prohibited under federal law from transportation on any aircraft. The indictment against defendant MEDCHEM Corporation was dismissed on Jun. 26, 2013. The

investigation was conducted by the FBI, Department of Commerce, IRS and Federal Aviation Administration.

***Military-Grade Thermal and Night Vision Goggles to the United Kingdom*** – On Jan. 28, 2014, Martin Gula a.k.a. Mark Welder, was charged by indictment in the Central District of California and on Dec. 12, 2013, by complaint in the District of Connecticut for violations of U.S. export control laws. According to court documents, between 2006 and 2013, Gula, a former member of the Slovakian Military Special Forces, used numerous fictitious names and an international network of suppliers, freight forwarders, mail forwarding companies, and bank accounts, to illegally export United States defense articles, including but not limited to military-grade thermal and night-vision goggles and scopes from the United States to the United Kingdom and various other European countries. On Dec. 18, 2013, the London Metropolitan Police Service arrested Gula in London, England, based upon a provisional arrest warrant in connection with Gula's involvement in violating United States export control laws. After he was charged by indictment in the Central District of California, Gula fled from England prior to extradition to the United States. Gula is currently a fugitive. This investigation was conducted by ICE.

***Firearms Parts to Thailand*** - On Jan. 24, 2014, two brothers, Nares Lekhakul and Naris Lekhakul, were sentenced in the Western District of Washington. Nares Lekhakul, a lawful permanent resident living in the State of Washington, was sentenced to two years in prison and three years of supervised release. His brother, Naris Lekhakul, a Thai citizen, was sentenced to three years in prison. The Lekhakul brothers were arrested in Jun. 2013, in connection with a conspiracy to illegally ship firearms parts to Thailand. In their Oct. 2013, plea agreements, the brothers admitted that Naris, while living in Thailand, identified the firearms parts he wanted ordered and shipped overseas. Initially the gun parts were sent to his brother Nares' home in Washington, where Nares attempted to disguise the shipments which were sent on to Thailand. After one shipment was seized in 2011, Naris recruited four other people to receive the shipments of firearms parts, disguise them, and send them on to Thailand. The co-conspirators did not obtain appropriate licenses to make the shipments. The co-conspirators would use fake names and fake invoices to try to avoid detection, and they packed various firearms parts in specific ways to try to avoid detection by x-ray scanners. Members of the group shipped various firearms parts with false labels. In all, the group is believed to be responsible for more than 250 shipments of restricted firearms components, worth more than \$750,000. The defendants did not ship any assembled firearms or entire firearms disassembled. The four codefendants previously pleaded guilty. In Dec. 2013, Witt Sittikornwanish and Sangsit Manowanna, U.S. citizens, were each sentenced to ten months in prison and Supanee Saenguthai, a Thai citizen residing in California, was sentenced to probation. Wimol Brumme, a Thai citizen residing in Nevada, was sentenced in Feb. 2014, to 7 months' imprisonment. This investigation was conducted by ICE HSI and the USPIS.

***Dual-Use Items to Pakistan Atomic Energy Commission*** – On Jan. 22, 2014, in the Middle District of Pennsylvania, a federal grand jury returned an Indictment against three individuals and two corporations, charging them with smuggling technology out of the United States for use by the Pakistan Atomic Energy Commission. The Indictment was unsealed on Mar. 31, 2014, after it was determined that none of the individuals were in the United States. The indictment alleged that Shafqat Rana, formerly of Lancaster, Pennsylvania, along with Abdul Qadeer Rana and Shahzad Rana, both of Lahore, Pakistan, used two corporations, Optima Plus International, a Pennsylvania corporation, and Afro Asian International, a Pakistani corporation, to export goods from the United States to Pakistan without first obtaining a license from the Department of Commerce. The goods were allegedly shipped through a common carrier in Dauphin County. Shafqat Rana allegedly took orders for dual-use items, that is, items with both a commercial and

military or nuclear application, from Afro Asian and acquired the items in the United States. After the items were shipped to Pakistan, they were resold to the Pakistan Atomic Energy Commission, an arm of the Pakistani Army, in violation of United States law. The Indictment charges that the defendants shipped and exported goods from the United States to restricted end-users in Pakistan while providing false and fraudulent invoices to the freight forwarders, thereby causing the freight forwarders to fail to file the required export declarations. The defendants also allegedly created false and misleading invoices given to freight forwarders that undervalued and mislabeled the goods and listed false purchasers and end-users of the goods. According to the United States Attorney's Office, Shafqat Rana left the United States and returned to Pakistan. This case was investigated by U.S. Department of Commerce and the FBI.

***Assault Weapon Parts and Gun Sights to Philippines*** - On Jan. 6, 2014, Romulo Arca Reclusado was sentenced in the Central District of California to 60 months' imprisonment, three years supervised release, a \$100 special assessment, and a \$7,500 fine. Previously, on Jun. 10, 2013, Reclusado pleaded guilty to conspiracy to violate the Arms Export Control Act and the International Emergency Economic Powers Act. On Feb. 7, 2011, in the District of Arizona, codefendant Mike Cabatingan also pleaded guilty to conspiracy. On Feb. 24, 2010, a federal grand jury in the Central District of California returned an indictment against Reclusado, Cabatingan, and Tirso Armando Aguayo for conspiring to illegally export defense articles and other controlled items from the United States to the Philippines. The defendants allegedly conspired to export to the Philippines molds used to make components for AR-15 assault rifles, as well as holographic rifle sights. Aguayo and Cabatingan were arrested on Feb. 25, 2010. On Jan. 12, 2011, the court granted a motion to dismiss the case against Aguayo. Reclusado was previously convicted in 1997 of conspiracy to transfer machine guns and illegally transferring machine guns for which he received a 27-month prison sentence. The investigation was conducted by ICE and DCIS.

***Commercial Industrial Machines to Iran*** - On Jan. 6, 2014, Mark Mason Alexander, a/k/a Musa Mahmood Ahmed, was sentenced in the Northern District of Georgia to 18 months in prison, followed by three years of supervised release and a \$100 special assessment. Alexander was found guilty by a jury on Sep. 26, 2013, of Conspiracy to violate the International Emergency Economic Powers Act. According to the charges and other information presented in court, between Oct. 2006, and Jun. 2008, Alexander conspired with two Iranian businessmen to sell Hydrajet water-jet cutting systems to customers located in Iran. Hydrajet Technology, located in Dalton, Ga., manufactured the water-jet cutting systems, which were used for the precision cutting of materials such as aluminum, glass, granite and steel. These machines were distributed to customers in the Middle East through Hydrajet Mena, another company that Alexander partly owned. Hydrajet Mena, for which Alexander was the CEO, was located in the United Arab Emirates. In 2007, as part of the conspiracy, Alexander negotiated the sale of two water-jet cutting systems to companies located in the Islamic Republic of Iran: The Parand Machine Company and the Negin Sanat Sadr. Company. In Jul. 2007, after Alexander negotiated the terms of these sales and before the machines were shipped to the Islamic Republic of Iran, the Department of Commerce conducted a community outreach meeting with Alexander, as the CEO of Hydrajet Technology. This outreach program was designed to make exporters like Alexander aware of the various export restrictions, including the trade embargo against Iran, and to educate exporters about the process for legally exporting items from the United States. The evidence further established that the machines that Alexander conspired to sell were in fact manufactured in Dalton, Ga. He concealed the true destination of these machines by causing them to be trans-shipped to the Islamic Republic of Iran via Alexander's company in the United Arab Emirates. Alexander additionally instructed Hydrajet Mena employees to travel to Islamic Republic of Iran to install the machines and to conduct software training for the Iranians who would operate them.

This case was investigated by the U.S. Department of Commerce and the Department of Homeland Security.

###